Wireless LAN Device Series

AP-G250

Multi-Function WLAN AP

User Manual

Version 1.0 (October 2008)

TABLE OF CONTENTS

SAFETY AND REGULATORY NOTICES 1

FCC STATEMENT 1
FCC CAUTION 1
FCC RF RADIATION EXPOSURE STATEMENT 1
CANADIAN DEPARTMENT OF COMMUNICATIONS INDUSTRY CANADA (IC) NOTICE 2

SAFETY GUIDELINES 2

PACKING LIST 3

PRODUCT OVERVIEW 4

FRONT VIEW 4
REAR VIEW 4

HARDWARE INSTALLATION 5

CONFIGURATION PREPARATION 5

HOW TO ACCESS CONFIGURATION AREA 5
BASIC LOGICAL PARTITIONING 5
DEFAULT IP ADDRESS 5
HOW TO SEE YOUR COMPUTER'S IP ADDRESS 6
HOW TO TEMPORARILY ASSIGN AN IP ADDRESS TO YOUR COMPUTER 6
ACCESSIBILITY TO CONFIGURATION VS. OPERATING MODE 11
DHCP 11

WIRELESS CONFIGURATION 12

OPERATION AND WIRELESS MODES 12
Operational Modes 12
Wireless Modes 12
OPERATIONAL MODES OVERVIEW 12
Router 12
Bridge 12
WISP (Wireless ISP) 13
WIRELESS MODES OVERVIEW 13
AP (Access Point) 13
Client 13
WDS (Wireless Distribution System) 13
WDS+AP 14
WIRELESS BASIC SETTINGS 14
Disable Wireless LAN Interface 14
Band 14
Mode 15
Network Type 15
SSID 16
Channel Number 16
Show Active Clients 17
Mac Clone (Single Ethernet Client) 17
Universal Repeater 18
WIRELESS ADVANCED SETTINGS 19
Authentication Type 20
Fragment Threshold 20
RTS Threshold 20
Beacon Interval 20
ACK Timing 21
Client Expired Time 21

MTU Size *21*
Data Rate *21*
Preamble Type *21*
Broadcast SSID *21*
IAPP (Inter-Access Point Protocol) *22*
802.11g Protection *22*
Block WLAN Relay (Isolate Client) *22*
Turbo Mode *22*
Transmit Power *22*
CONFIGURING WIRELESS SECURITY 23
WEP Encryption Setting *23*
WEP Encryption with 802.1x Setting *25*
WPA Authentication Mode *26*
WIRELESS ACCESS CONTROL 27
WDS 27
WDS Network Topology *28*
WDS Application *32*
Site Survey *33*
Connecting Profile *34*

TCP/IP CONFIGURATION 36

LAN INTERFACE 36
Default Gateway *36*
DHCP Server *36*
DHCP Client Range *37*
WAN INTERFACE 38
Static IP *39*
DHCP Client (Dynamic IP) *40*
PPPoE *41*
PPTP *42*
Configuring Clone MAC Address *43*
VPN Pass-through *45*
ROUTE 46
NAT (Network Address Translation) *46*
IP Forwarding Default Policy *47*
Static Route Setup *47*
Dynamic Route Setup *48*

FIREWALL CONFIGURATION 50

CONFIGURING LAN TO WAN FIREWALL 50
PORT FILTERING 50
IP FILTERING 51
MAC FILTERING 52
CONFIGURING PORT FORWARDING (VIRTUAL SERVER) 53
Multiple Servers behind NAT (Example) *54*
CONFIGURING DMZ 55
CONFIGURING VPN 56

MANAGEMENT 57

STATUS 57
QUALITY OF SERVICE (QOS) 58
BANDWIDTH CONTROL 61
SNMP AGENT 62
STATISTICS 65
TIME ZONE SETTING 65
LOG 66
MISCELLANEOUS SETTINGS 66
HTTP Port *66*
PING WATCHDOG 67

MESH NETWORK 68
UPGRADE FIRMWARE 74
Firmware Overview *74*
Firmware Upgrade Procedure *74*
Save/Reload Settings *75*
Password *76*

USING CLI MENU 77

START A SSH (SECURE SHELL) CLIENT SESSION 77
EXECUTE CLI PROGRAM 77

AUTO-DISCOVERY TOOL 79

TROUBLESHOOTING 81

Basics *81*
Power Light Not On *81*
Ethernet Light (LED) Not On *81*
Web Browser Configuration Screen Not Available *81*
Configuration Changes Not Saved *82*
No Internet Access *82*
Troubleshooting a TCP/IP Network Using a Ping Utility *85*
Testing the Path from Your Computer to a Remote Device *86*

APPENDIX A 87

TECHNICAL SPECIFICATIONS 87

APPENDIX B 91

BASIC WIRELESS BRIDGED ACCESS POINT 91
BASIC WIRELESS ROUTER 91
UNIVERSAL REPEATER MODE 91
WDS OR WDS+AP MODE 92
CLIENT MODE 92

SAFETY AND REGULATORY NOTICES

FCC Statement

The AP-G250 Access Point has been tested and found to comply with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference
- This device must accept any interference received, including interference that may cause undesired operation.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

FCC Caution

Any change of modification to the product not expressly approved by AIR802 could void the user's authority to operate the device.

FCC RF Radiation Exposure Statement

To comply with the FCC rules 47 CFR 1.1307 and ANSI C95.1 RF exposure limits, the antenna(s) for this device must comply with the following:

A minimum separation distance of at least 20cm (8 inches) is required between the antenna and all persons.

Canadian Department of Communications Industry Canada (IC) Notice

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 et CNR-210 du Canada.

Safety Guidelines

- Do not touch or move antenna(s) while the unit is transmitting or receiving.
- Do not hold any component containing a radio such that the antenna is very close to or touching any exposed parts of the body, especially the face and eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; otherwise the radio may be damaged.
- Antenna selection and installation should follow the rules of the country in which the device is being installed. Professional installation is recommended.

PACKING LIST

Before you start to install the AP-G250, make sure the package contains the following items

- AP-G250 unit
- Antenna
- Power Supply
- Ethernet Network Cable
- CD

PRODUCT OVERVIEW

Front View

Rear View

1. Power supply connector
2. WAN/LAN Connector – This port can be used as a WAN interface that connects to a DSL or Cable Modem, or as a LAN port for connection to a computer, printer or other networked device.
3. LAN Port – This port connects a computer, printer or other networked device.
4. Reset Button

HARDWARE INSTALLATION

Once you have ensured that you have all required components, you can install the AP-G250.

1. Connect the Ethernet network cable between the WAN/LAN Interface Connector at the rear of the AP and your network. The network connection may be a cable or DSL modem, existing router or other device. For some applications, a cable is not required.
2. Connect the power supply to the Power Supply Connector to the rear of the AP and to the power outlet.
3. Connect another Ethernet network cable (not supplied with the AP) between the LAN Interface Connector and a computer or other network device, as required.
4. Initial configuration can be performed using the wired LAN port or via wireless connection.

You can now proceed to use the computer to configure the AP-G250.

CONFIGURATION PREPARATION

How to Access Configuration Area

There are two ways to configure the device:

1. Using a web-browser, such as Internet Explorer.
2. Using a Secure Shell CLI Interface.

Basic Logical Partitioning

For many first time users, it might be useful to consider the AP-G250 as having two logical sections: a wired Ethernet network interface (NIC) and an 802.11b/g wireless network interface (NIC). Each interface has its own MAC address.

Default IP Address

The AP-G250 has a default LAN IP address of 192.168.2.254 and a subnet-mask address of 255.255.255.0. To access the AP-G250 configuration, you must first ensure that your computer's IP address is on the same subnet (192.168.2.X) as the default IP

address. For example, you can assign your computer an IP address of 192.168.2.200. Do not assign 192.168.2.254 (this is the IP address of the AP-G250).

Your computer probably is set to “Obtain IP Address Automatically”. If the last IP address was on another network, such as 192.168.1.200, then you will not be able to connect without temporarily assigning your computer an IP address in the same subnet.

Typically, the AP-G250 is accessed via the LAN or wireless interface, however if you need to access the AP-G250 via the WAN interface, the default IP address is 172.1.1.1 and you will need to ensure that you are on the same subnet (172.1.1.X).

How to See Your Computer’s IP Address

For a Windows-based computer, follow these steps:

1. Click Start > Run.
2. Type CMD in the Open: field and click OK.
3. Type ipconfig at the cursor prompt and press Enter.
4. Scroll to Ethernet Adapter Local Area Connection and note the listing for IP address.

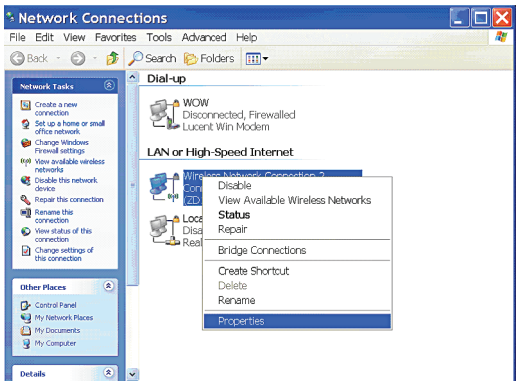
How to Temporarily Assign an IP Address to Your Computer

The following example illustrates the procedure for statically assigning an IP address in the same subnet as the default address.

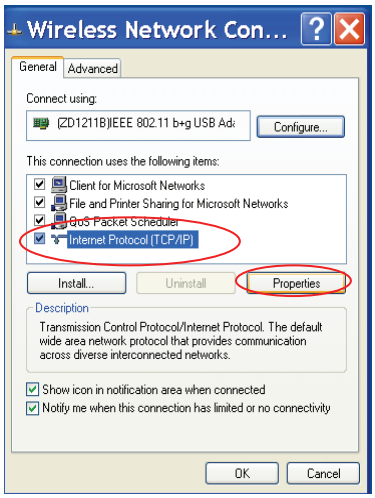
Windows XP

1. Click **Start**, right click **My Network Places** and click **Properties**.

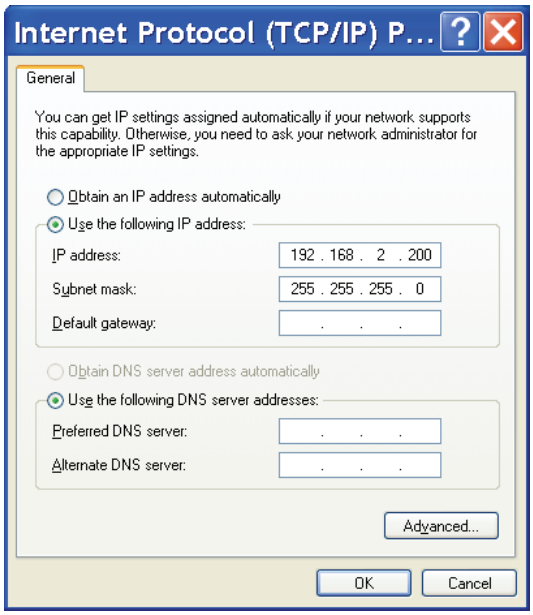
2. Right click either **Local Area Connection** or **Wireless Network Connection**, depending on how you are accessing the AP-G250 (by an Ethernet network cable or via a wireless card), and select **Properties**.



3. Select **Internet Protocol (TCP/IP)** and click **Properties**.



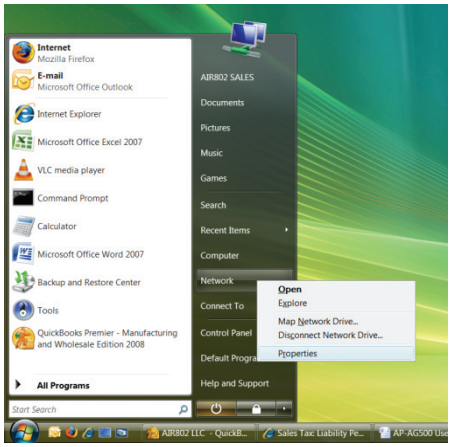
4. Click the button to select **Use the following IP address**. Enter a Static IP Address in the same subnet as the Default IP Address.


Internet Protocol (TCP/IP) P...
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 2 . 200
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

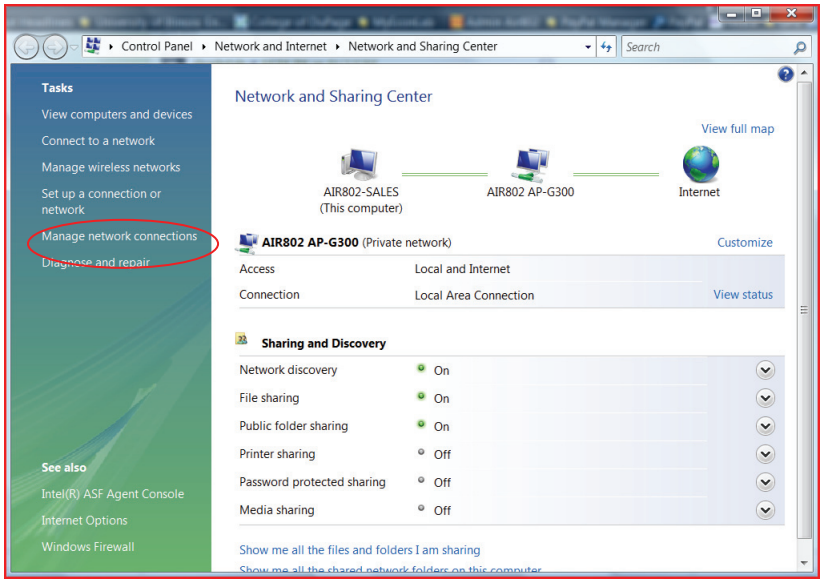
5. Click **OK**.

Windows VISTA

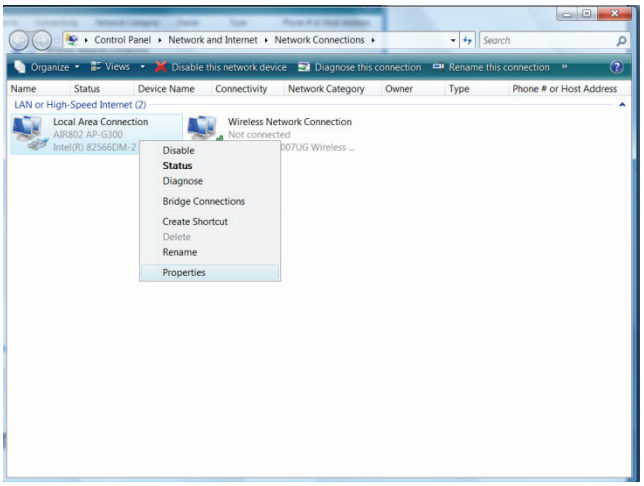
1. Click **Start**, right click **Network** and choose **Properties.** The Network and Sharing Center opens.



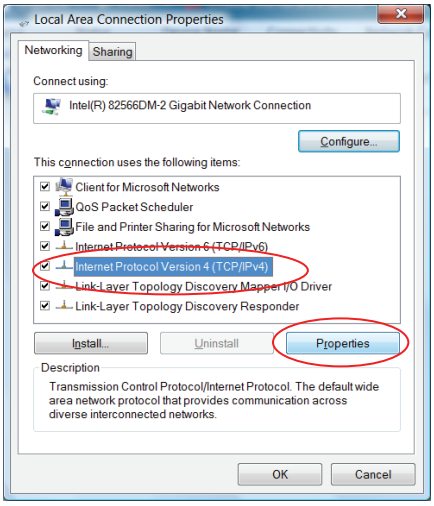
2. Select **Manage Network Connections** from the left sidebar.



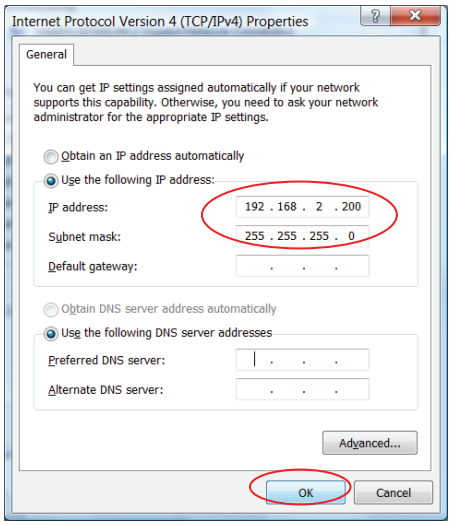
3. Right click either **Local Area Connection** or **Wireless Network Connection**, depending on how you are accessing the AP-G250 (by an Ethernet network cable or via a wireless card), and select Properties.



4. Click **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



6. Click the button to select **Use the following IP address**. Enter a Static IP Address in the same subnet as the Default IP Address.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 2 . 200
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

7. Click **OK**, and **OK** again in the previous Connection Properties window.

Accessibility to Configuration vs. Operating Mode

The AP-G250 has three operation modes: Router, Bridge and WISP (see Wireless Configuration for a detailed explanation). Accessibility to the AP-G250's LAN interface depends on the current mode of operation, as shown in the following table:

CONFIGURATION ACCESSIBILITY CHART

Operating Mode	WLAN	WIRED LAN	WAN
Router	YES	NO	YES
Bridge(AP Client)	YES	YES	NO
WISP	YES	YES	YES

For example, if the AP-G250 is operating in Router mode and you try to access the AP-G250 IP address from the wired Ethernet LAN connection, you will not succeed since NAT will be enabled.

DHCP

By default, the DHCP server is operational. If you are connecting the AP-G250 in Bridge mode into a wired router with DHCP running, you need to change the DHCP server setting. Multiple DHCP servers running in the network will result in conflicts. In this event, change DHCP to either disabled or client.

Note: If you change DHCP to client, it will obtain its IP address from the upstream DHCP server (this could be a consumer grade broadband router to which the AP-G250 is connected). If you change DHCP to disabled, it will use the IP address assigned by you or the default IP address.

Auto-Discovery Tool

The CD included in the AP-G250 package contains the manual and an auto-discovery tool. This tool is very useful if you've forgotten the IP address of the AP-G250 or are configuring a previously installed access point with an unknown device address. It will discover the IP address even if your computer is not in the same subnet as the AP-G250. See Auto-Discovery Tool for more information.

WIRELESS CONFIGURATION

The AP-G250 configuration software includes a Wizard that assists you in making most basic changes. Alternatively, instead of using the Wizard or if you need changes to functions that the Wizard does not allow you to change, click on the various file folders.

Operation and Wireless Modes

Operational Modes

The AP-G250 has three possible operational modes to choose from:

- Router
- Bridge
- WISP (Wireless ISP)

Note: The operational mode relates to the communication between the wired Ethernet network interface card (NIC) and the wireless NIC.

Wireless Modes

The wireless radio interface has four possible modes to choose from:

- AP (Access Point)
- Client
- WDS (Wireless Distribution System)
- WDS + Access Point

Operational Modes Overview

Router

The wired Ethernet (WAN) port is used to connect with an ADSL/Cable modem or router and the wireless network interface (NIC) is used for your private wireless local area network (WLAN). Network address Translation (NAT) exists between the wired Ethernet network interface and the wireless network interface. All wireless clients share the same public IP address (provided through the cable or DSL modem) through the WAN port to the ISP. The default IP configuration for the WAN port is static IP. You can access the web server of the device through the default WAN IP address 172.1.1.1 and modify the setting to DHCP client or other options based on your ISP requirement.

Bridge

When this mode is selected, the wired Ethernet and wireless NIC are bridged together and all the WAN related functions are disabled. This mode is the most common and is

the default operational mode. It is often used when the AP-G250 is being wired to an existing router or switch. When using Bridge mode, the LAN IP address can be accessed via the wired or wireless interface.

WISP (Wireless ISP)

This mode lets you access the access point of your wireless ISP or connect to any available wireless network and share the same public IP address from your ISP or wireless service with the PCs connecting with the wired Ethernet port of the AP-G250. In this mode, the Ethernet port will often be connected to another wireless router.

To use this mode, you must first set the wireless radio to client mode and connect to the AP (access point) of your ISP. Then you can configure the WAN IP configuration to meet your ISP requirements.

Wireless Modes Overview

AP (Access Point)

In this mode, the wireless radio of the AP-G250 serves as communications “hub” for wireless clients and provides a connection to a wired LAN.

Client

This mode provides the capability to connect with another access point using infrastructure/Ad-hoc networking. With bridge operation mode, you can directly connect the wired Ethernet port to your PC and the AP-G250 becomes a wireless client or adapter. With WISP operation mode (NAT is enabled), you can connect the wired Ethernet port to a hub/switch and all the PCs connecting with the hub/switch can share the same public IP address from your ISP.

WDS (Wireless Distribution System)

This mode serves as a wireless repeater. The AP-G250 forwards the packets to another AP with WDS function. When this mode is selected, it is not broadcasting an SSID and wireless clients can’t survey and connect to the device.

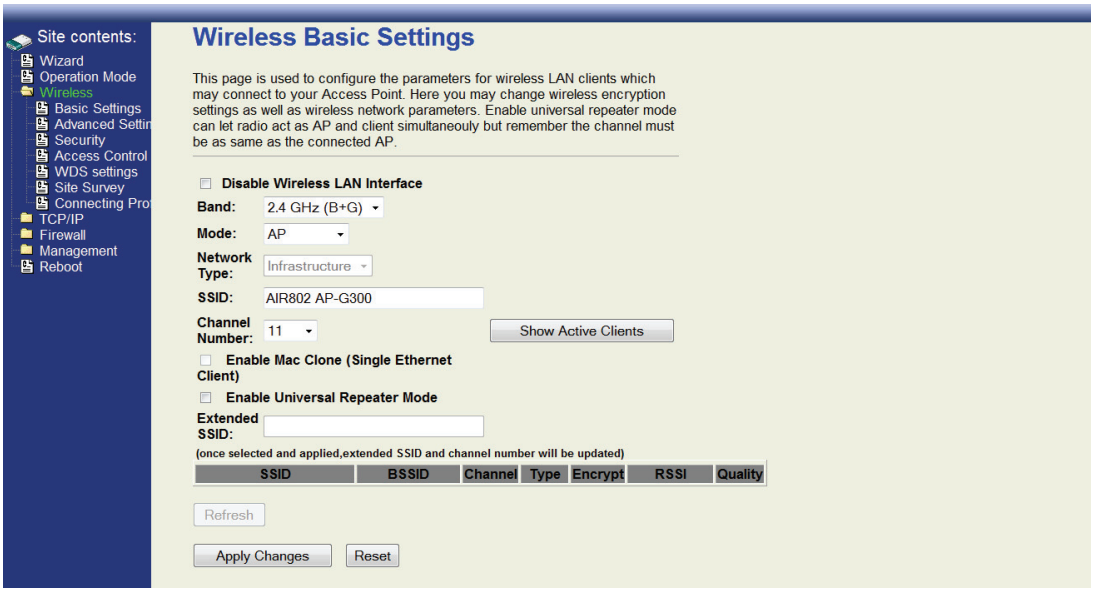
WDS+AP

This mode combines WDS and AP modes, allowing WDS connections and letting wireless clients survey and connect to the device.

Table of Operational and Wireless Mode Combinations

	Bridge	*Router*	*WISP*
AP	YES	YES	NO
WDS	YES	YES	NO
Client	YES	NO	YES
AP+WDS	YES	YES	NO

Wireless Basic Settings



Disable Wireless LAN Interface

Checking this will disable the wireless LAN interface. This would not ordinarily be disabled.

Band

The options are: 802.11b, 802.11g or 802.11b/g. Default is 802.11b/g.

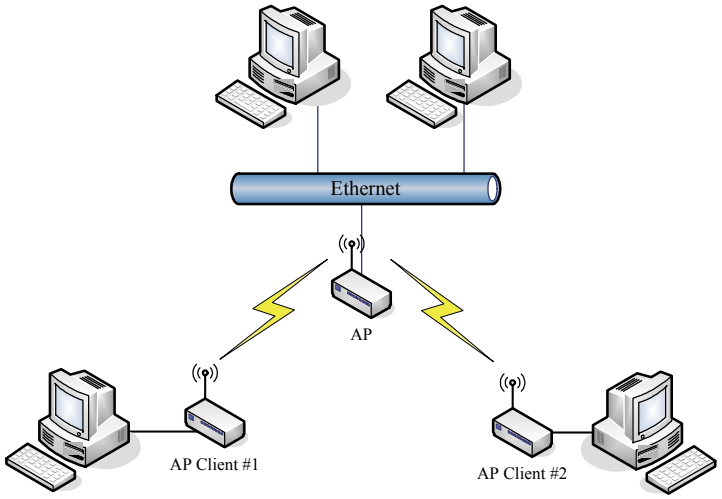
Mode

The modes selectable are: AP, Client, WDS, WDS+AP. See the full description and details of each of these in the preceding section.

Network Type

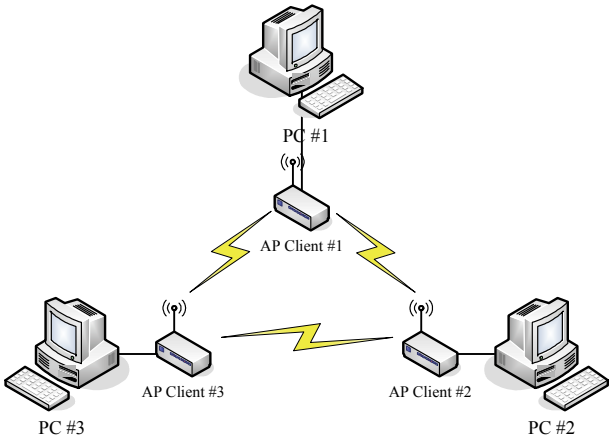
1. Infrastructure

This network type requires the presence of an 802.11b/g Access Point. All communication is done via the AP.



2. Ad Hoc

This type provides a peer-to-peer communication between wireless stations. All the communication is done from Client to Client without any Access Point involved. Ad Hoc networking must use the same SSID and channel for establishing the wireless connection.



In client mode, the AP-G250 doesn't support Router mode functions, including Firewall and WAN settings.

SSID

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access point/bridges on a network or sub-network can use the same SSID. SSIDs are case sensitive and can contain up to 32 alphanumeric characters.

Channel Number

The following table lists the available frequencies (in MHz) for the 2.4 GHz radio:

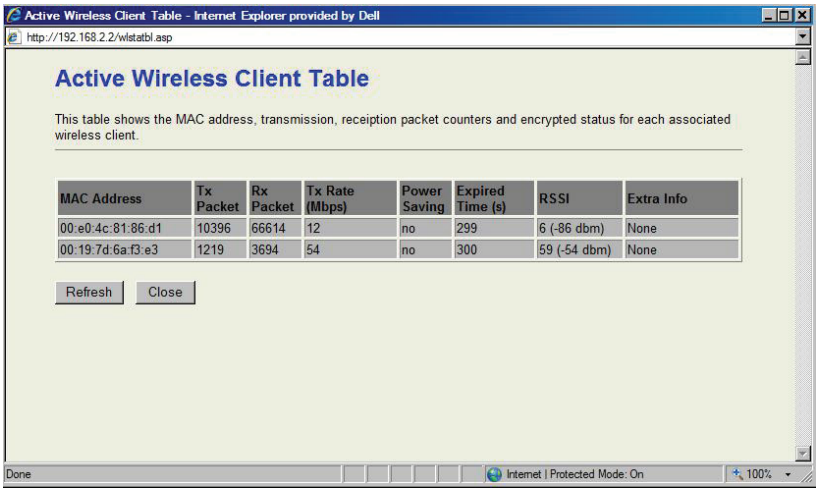
Channel No.	Frequency	Country Domain
1	2412	Americas, EMEA, Japan and China
2	2417	Americas, EMEA, Japan and China
3	2422	Americas, EMEA, Japan, Israel and China
4	2427	Americas, EMEA, Japan, Israel and China
5	2432	Americas, EMEA, Japan, Israel and China
6	2437	Americas, EMEA, Japan, Israel and China
7	2442	Americas, EMEA, Japan, Israel and China
8	2447	Americas, EMEA, Japan, Israel and China
9	2452	Americas, EMEA, Japan, Israel and China
10	2457	Americas, EMEA, Japan and China
11	2462	Americas, EMEA, Japan and China
12	2467	EMEA and Japan only
13	2472	EMEA and Japan only
14	2484	Japan only

Note: The system ships with channels 1 through 11 enabled. If you are located in a country that allows channels 12, 13 and 14, you can contact AIR802 for information on enabling the additional channels.

When Channel Number is set to **Auto**, the AP-G250 will find the least-congested channel for use.

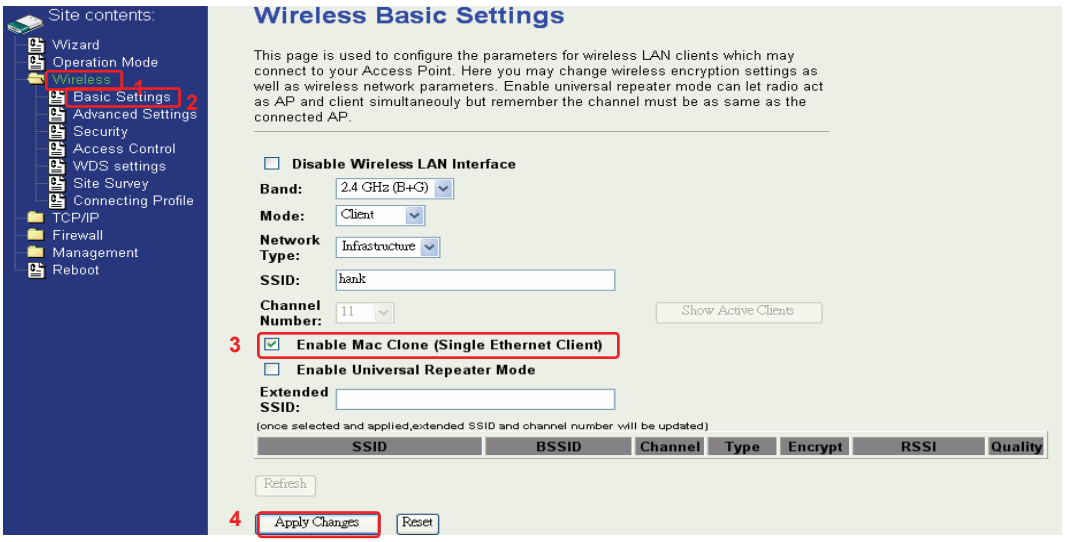
Show Active Clients

Click **Show Active Clients** to view a table of all active clients connected to the access point. Useful information such as the as MAC address, transmission information and signal level is provided.



Mac Clone (Single Ethernet Client)

When MAC Clone is enabled, the Ethernet client (for example, your computer) uses its own MAC address to transmit data. When MAC Clone is disabled, the single Ethernet client must to use the AP-Client's MAC address.



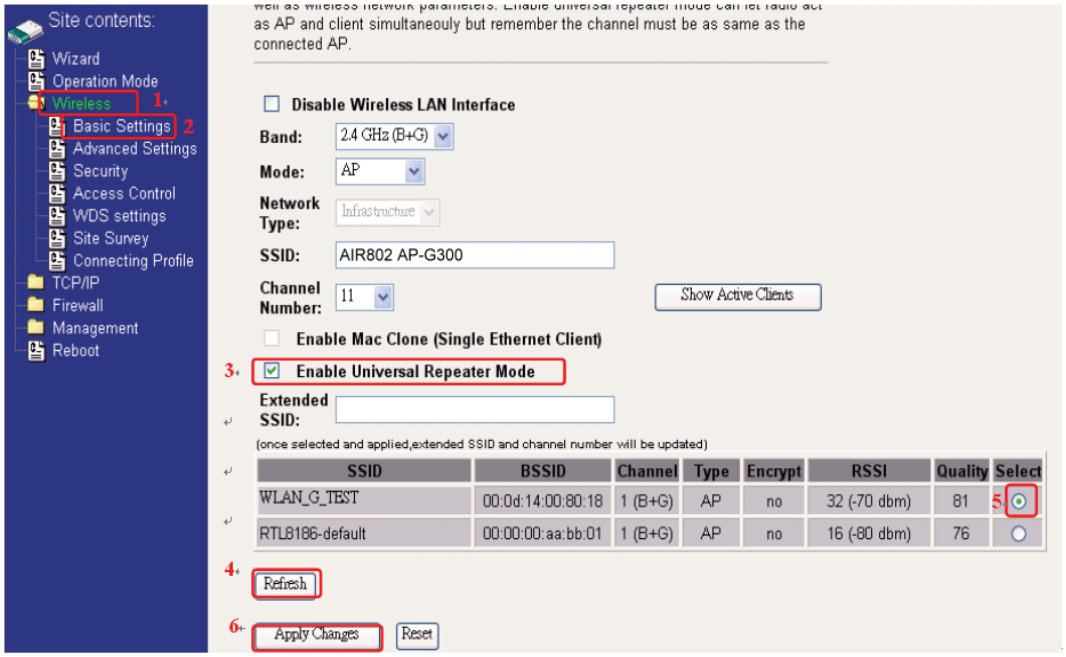
NOTE: This function is not used in most applications.

Universal Repeater

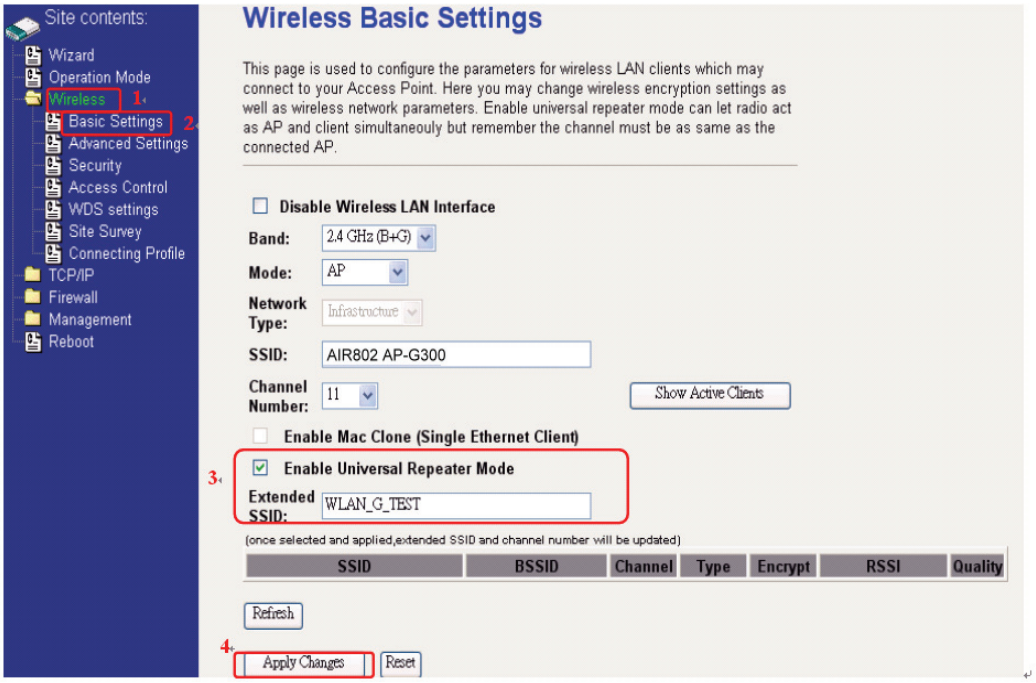
. In this mode, the AP-G250 can be configured as a repeater to connect to another AP and simultaneously re-broadcast the signal locally. Essentially, this will extend the available wireless range of another AP and let the user link to the network that they want. It will perform as an AP and repeater simultaneously, versus WDS or WDS+AP mode where you enter the MAC address of any device communicating with the other. If you control the remote AP, then WDS may be preferable. If you do not control or own the remote AP, then Universal Repeater is the correct choice.

To configure Universal Repeater:

1. Click **Enable Universal Repeater Mode**
2. Click **Refresh** to show the available SSIDs.
3. Select an SSID by clicking the **Select** button on the far right.
4. Click **Apply Changes**.



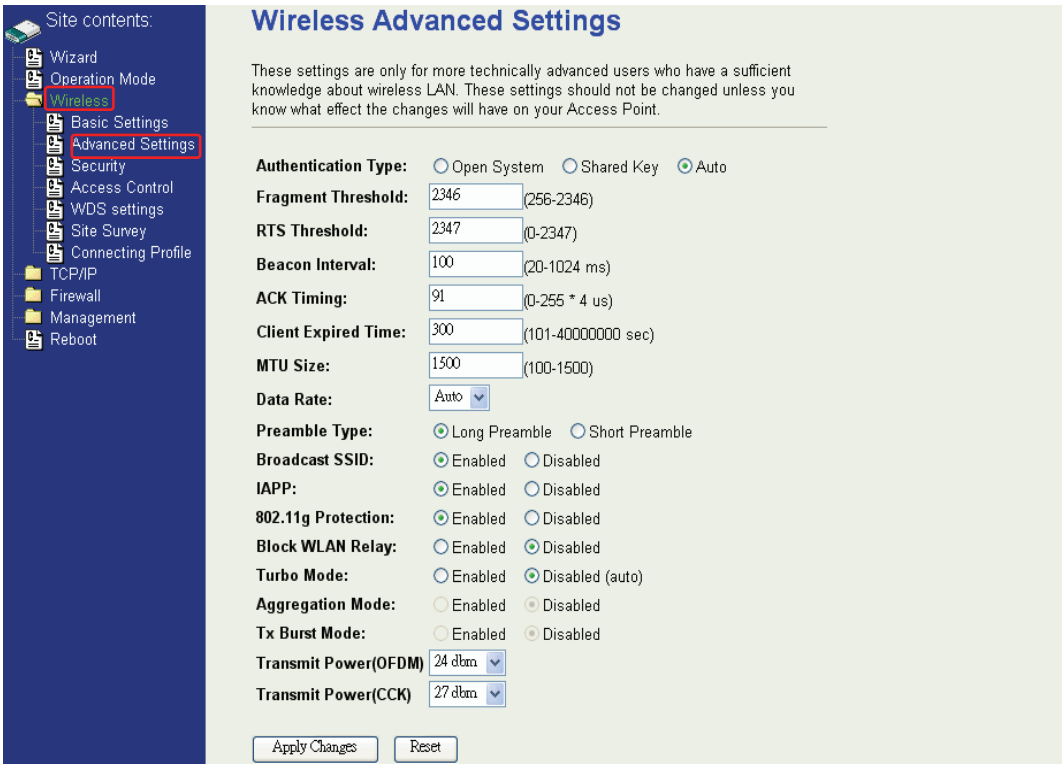
The following screen shows the Extended SSID is filled in after selecting the desired network (SSID) above.



Wireless Advanced Settings

These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your device. The default settings are optimized for normal operation.

Note: Any unreasonable value change to a default setting will reduce the throughput of the device.


Site contents:
Wizard
Operation Mode
Wireless
Basic Settings
Advanced Settings
Security
Access Control
WDS settings
Site Survey
Connecting Profile
TCP/IP
Firewall
Management
Reboot
Wireless Advanced Settings
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.
Authentication Type: Open System Shared Key Auto
Fragment Threshold: 2346 (256-2346)
RTS Threshold: 2347 (0-2347)
Beacon Interval: 100 (20-1024 ms)
ACK Timing: 91 (0-255 * 4 us)
Client Expired Time: 300 (101-40000000 sec)
MTU Size: 1500 (100-1500)
Data Rate: Auto
Preamble Type: Long Preamble Short Preamble
Broadcast SSID: Enabled Disabled
IAPP: Enabled Disabled
802.11g Protection: Enabled Disabled
Block WLAN Relay: Enabled Disabled
Turbo Mode: Enabled Disabled (auto)
Aggregation Mode: Enabled Disabled
Tx Burst Mode: Enabled Disabled
Transmit Power(OFDM) 24 dbm
Transmit Power(CCK) 27 dbm
Apply Changes
Reset

Authentication Type

Wireless clients can associate with the AP-G250 using either “Open system” or “Shared Key” Authentication. If “Shared Key” is selected, you need to configure “WEP key” on the “Security” page (See the next section). The default setting is “Auto”.

Fragment Threshold

The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference. This function will help improve network performance.

RTS Threshold

The RTS threshold determines the packet size at which the radio issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the device, or in areas where the clients are far apart and can detect only the AP-G250 and not each other. You can enter a setting ranging from 0 to 2347 bytes.

Beacon Interval

The beacon interval is the amount of time between access point beacons in milliseconds. The default beacon interval is 100.

ACK Timing

Acknowledgement Timing is the amount of time that the AP waits for the client's response. This concept is related to EIFS (Extended Inter-Frame Space). The EIFS interval begins while the device is idle after detection of an erroneous frame. The EIFS is defined to provide enough time for another device to acknowledge what was, to this device, an incorrectly received frame before this device commences transmission.

ACK timing range can be set from 0 TO 255 (0 is the default). The higher the ACK timing, the lower the throughput will be. If set too high, packets can be lost as the router waits for the ACK window to timeout. Conversely, if ACK is set too low, the window will expire too soon and returning packets can be dropped, also lowering throughput.

Client Expired Time

The client expired time determines the time interval the client need to re-associate with the device while the client is idle. The default client expired time is 300 seconds.

MTU Size

The MTU (Maximum Transmission Unit) setting controls the maximum Ethernet packet size your PC will send. A limit is required because ISPs and Internet backbone routers and equipment will fragment any packet larger than their limit, then these parts are re-assembled by the target equipment before reading. You may need to change the MTU for optimal performance of your wireless LAN traffic. The default MTU size is 1500

Data Rate

The standard IEEE 802.11b communication supports 11, 5.5, 2 and 1 Mbps data rates. The standard IEEE 802.11g communication supports 54, 48. 36, 24, 12, 9 and 6 Mbps data rates. You can choose the rate that the device uses for data transmission. The default value "auto" lets the device select the highest possible transmission rate.

Preamble Type

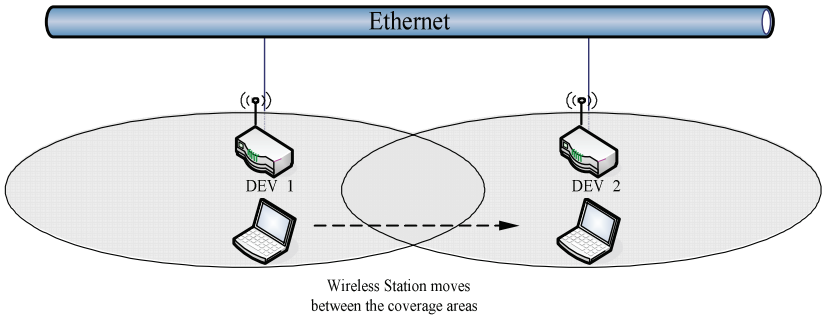
The preamble is part of the 802.11 frame and is PHY dependent. All 802.11b/g equipment supports the long preamble. The short preamble (optional) maybe used to improve throughput when all stations on the network support the short preamble.

Broadcast SSID

Broadcasting the SSID will let your wireless clients find the device automatically. If you are building a public wireless network, disabling this function can improve security. Every wireless stations located within the coverage of the device must connect this device by manually configure the SSID in the client settings.

IAPP (Inter-Access Point Protocol)

This function lets wireless stations roam in a network environment with multiple devices. Wireless Stations can switch from one device to another as they move between coverage areas, extending the wireless working range.



Note: To implement the roaming function, settings MUST comply with the following:

- All devices must be in the same subnet network and the SSID must be the same.
- If you use 802.1x authentication, you need to have the user profile in these devices for the roaming station.

802.11g Protection

This ensures that 802.11g stations are backward compatible with legacy 802.11b stations. With 802.11g protection enabled, a CTS will be used to lock out 802.11b stations while the 802.11g station is transmitting. It should be disabled in a pure 802.11g environment, as it will have a significant impact on 802.11g performance (as high as 50% decrease in throughput).

Block WLAN Relay (Isolate Client)

If you are building a public Wireless Network, enabling this isolation function can provide better security. The device will block packets between wireless clients (relay). All the wireless clients connected to the device can't see each other.

Turbo Mode

This allows two devices or stations using Realtek 802.11b/g chipsets to transmit at 72Mbps between each other. Note that this function is proprietary and will only function between Realtek stations.

Transmit Power

The device supports five transmission output power levels from 20 to 24dBm for CCK (802.11b) mode and four transmission output power levels from 17 to 20dBm for OFDM

(802.11g) mode. You can adjust the power level to change the coverage of the device. For best results, wireless client devices should have similar power output to allow bi-directional communication with the AP-G250.

Configuring Wireless Security

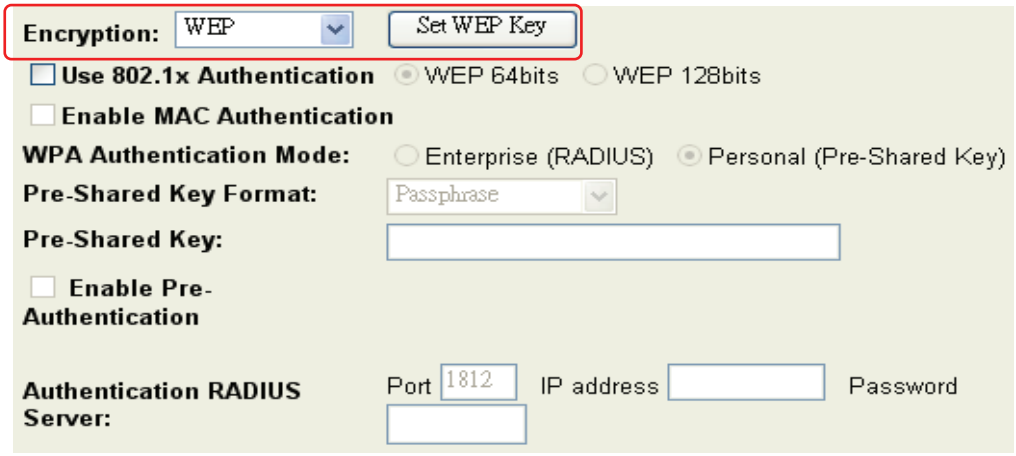
The AP-G250 provides complete wireless security functions, including WEP, 802.1x, WPA-TKIP, WPA2-AES and WPA2-Mixed. The default security setting is all security modes disabled.

WEP Encryption Setting

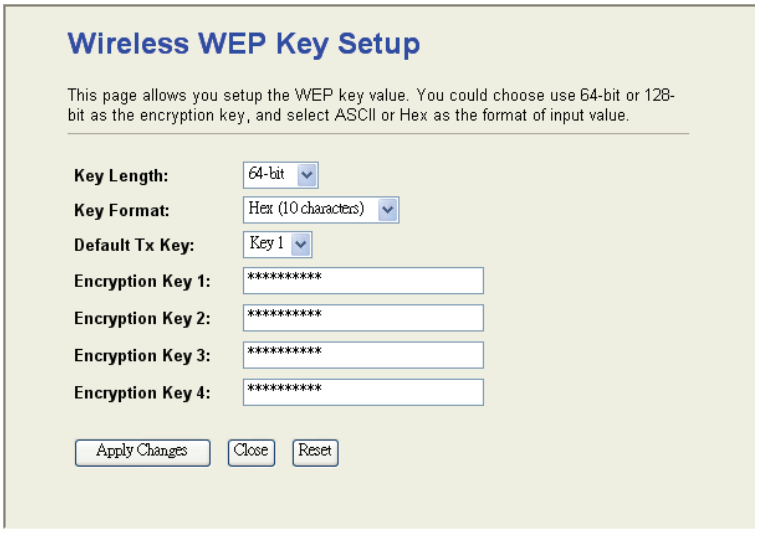
Wired Equivalent Privacy (WEP) is the easiest and most basic security level to implement. The WEP setting must be as same as each client in your wireless network. To use WEP:

1. Change the encryption type to **WEP**.

2. Click **Set WEP Key** to open the “Wireless WEP Key setup” page.

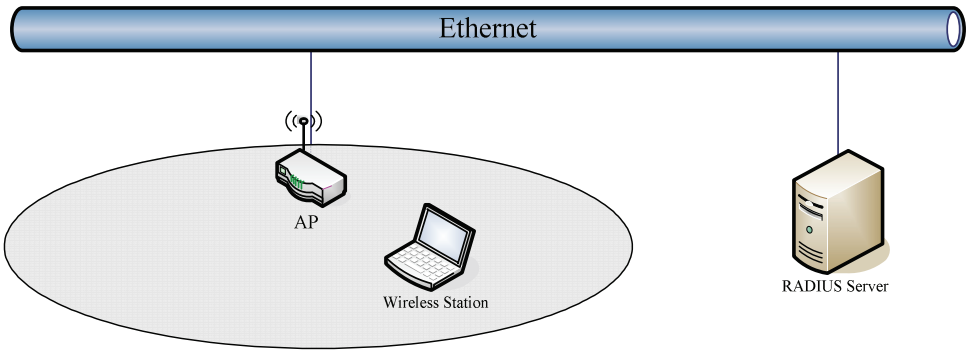


3. Choose a Key Length and Key Format. For 40-bit and 64-bit keys you can input 10 hexadecimal digits (0~9, a~f or A~F) or 5 ACSII characters. For 104-bit and 128-bit WEP keys you can input 26 hexadecimal digits (0~9, a~f or A~F) or 10 ACSII characters.
4. The Default Tx Key field decides which of the four keys you want to currently use in your WLAN environment. Typically only one key is used, the default key or Key 1.
5. For each key you want to enter, use the backspace key to clear the entry field and type into the space a key that matches the selected length and format.

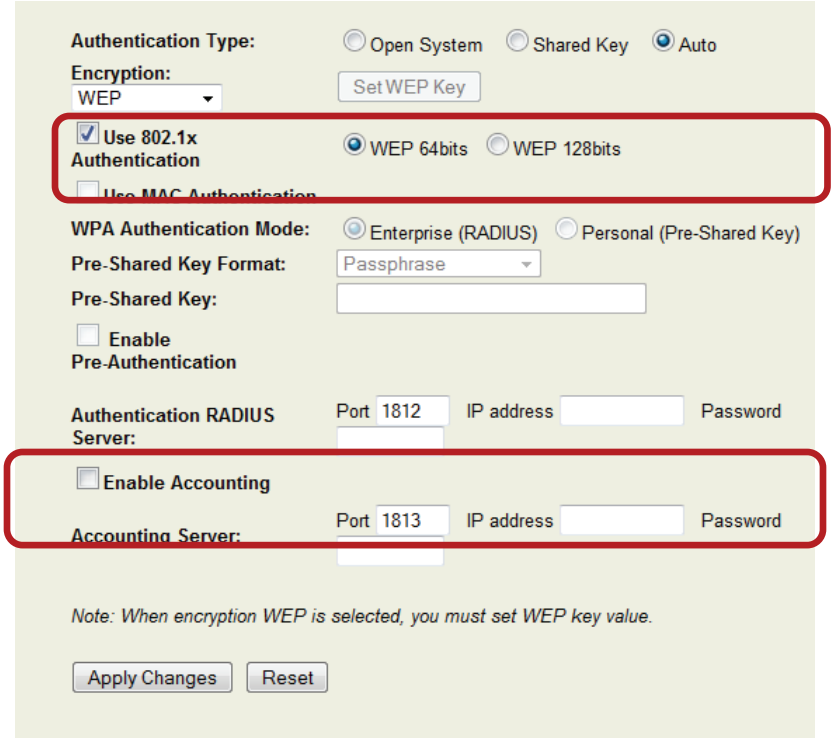

Wireless WEP Key Setup
This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.
Key Length: 64-bit
Key Format: Hex (10 characters)
Default Tx Key: Key 1
Encryption Key 1: **********
Encryption Key 2: **********
Encryption Key 3: **********
Encryption Key 4: **********
Apply Changes
Close
Reset

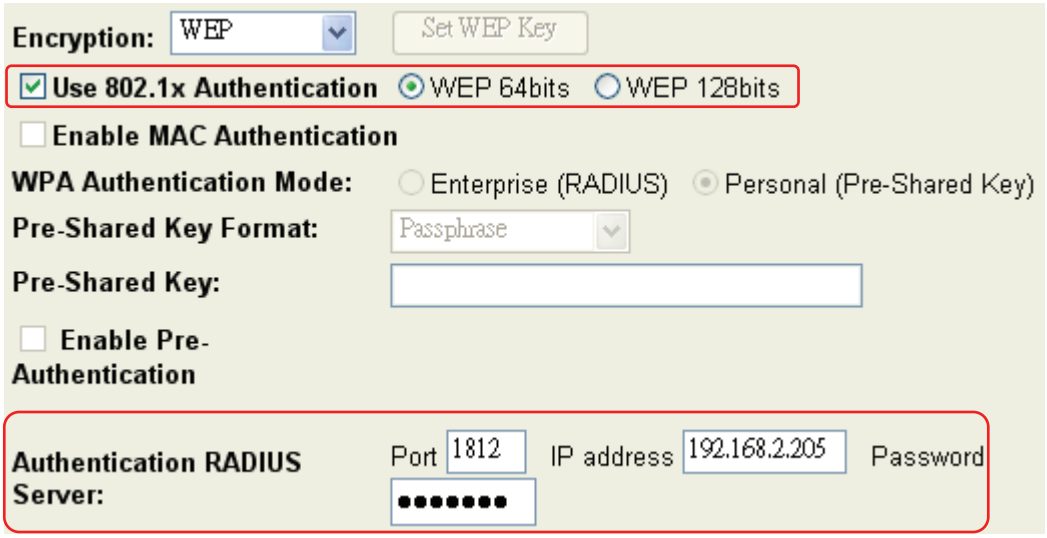
WEP Encryption with 802.1x Setting

The AP-G250 supports an external RADIUS Server or other authentication server that can secure networks against unauthorized access. If you use WEP encryption, you can use the RADIUS server to control user admission. Every user must have a valid account before accessing the Wireless LAN. An example is as follows:



Choose WEP 64 or 128 bit encryption based on your current network requirements. Then add user accounts and the target device to the RADIUS server. In the AP-G250, specify the IP address, Password (Shared Secret) and Port number of the target RADIUS server.





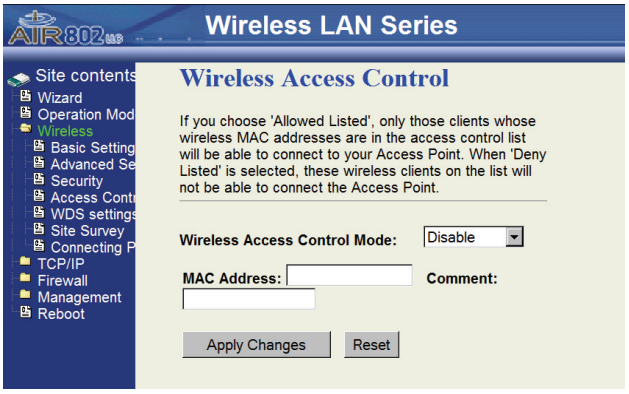
WPA Authentication Mode

WPA authentication provides a high level of assurance that data will remain private and network access will be restricted to authorized users. To use WPA authentication:

1. Change the encryption type to **WEP**.
2. Select an Authentication Mode. The AP-G250 supports two WPA modes:
    - **Enterprise (RADIUS):** In this mode authentication is achieved using a WPA RADIUS Server or other authentication server on the network. You have to add user accounts and the target device to the RADIUS Server. In the AP-G250, you need to specify the IP address, Password (Shared Secret) and Port number of the target RADIUS server.
    - **PSK (Pre-Share Key):** This mode requires only an access point and client station that supports WPA-PSK. The WPA-PSK settings for Key Format, Length and Value must be the same for each wireless client in your wireless network. When Key Format is Passphrase, the key value must have 8~63 ACSII characters. When Key Format is Hex, the key value must have 64 hexadecimal digits (0~9, a~f or A~F).

Wireless Access Control

Wireless Access Control by default is disabled. You may choose to Allow Listed or Deny Listed. The MAC addresses inserted will then be used to either allow or deny entry by wireless client devices thus controlling access by the user's MAC addresses.



WDS

Wireless Distribution System (WDS) uses wireless media to connect one or more remote LANs with the local LAN in applications such as building to building network extensions, wireless IP camera video surveillance networks, and wireless network extension where one AP is connected to the Internet and multiple other AP's communicate wirelessly with the first AP while simultaneously providing wireless service.

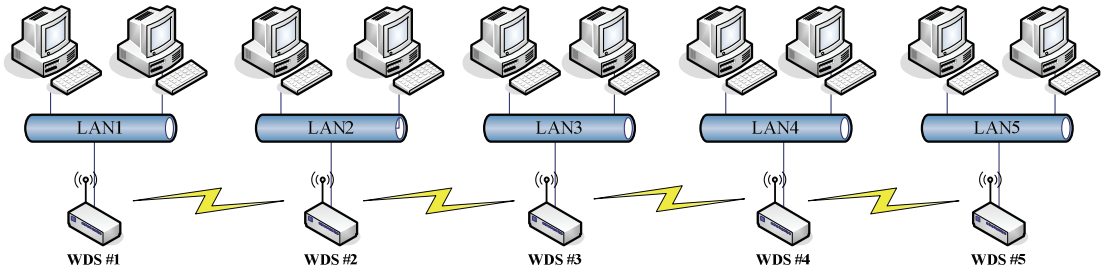
To use WDS to extend your WLAN, the following conditions apply:

- The bridging devices in a WDS network must use the same radio channel.
- When WDS only mode is enabled, no SSID is broadcast so no wireless stations can connect (they can connect in AP+WDS mode).
- If your network topology has a loop, the 802.1d Spanning Tree function must be enabled. The default setting is enabled.
- Any AP communicating directly with another AP must have the wireless MAC address entered in the WDS MAC table under WDS Settings Page. Each AP communicating directly with another AP must know about each other's MAC address. You don't need to add all MAC address of devices existing in your network to the WDS List; only the address of devices you need to directly connect to.
- Bandwidth will be shared between bridging devices. The maximum number of devices is eight in the WDS network.

WDS Network Topology

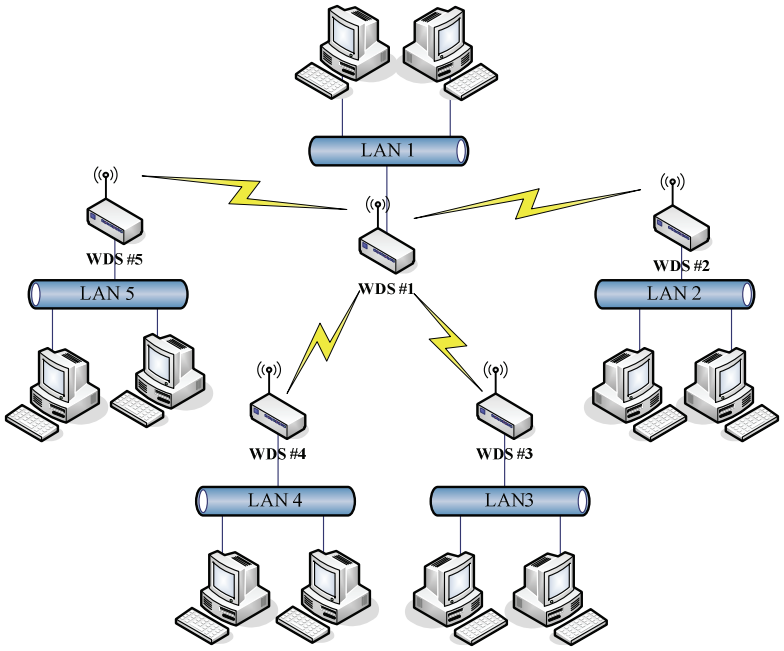
This section details WDS network topologies and WDS List configuration. You can set up four kinds of network topologies: bus, star, ring and mesh. In this case, there are five devices with WDS enabled: WDS1, WDS2, WDS3, WDS4 and WDS5.

Bus topology



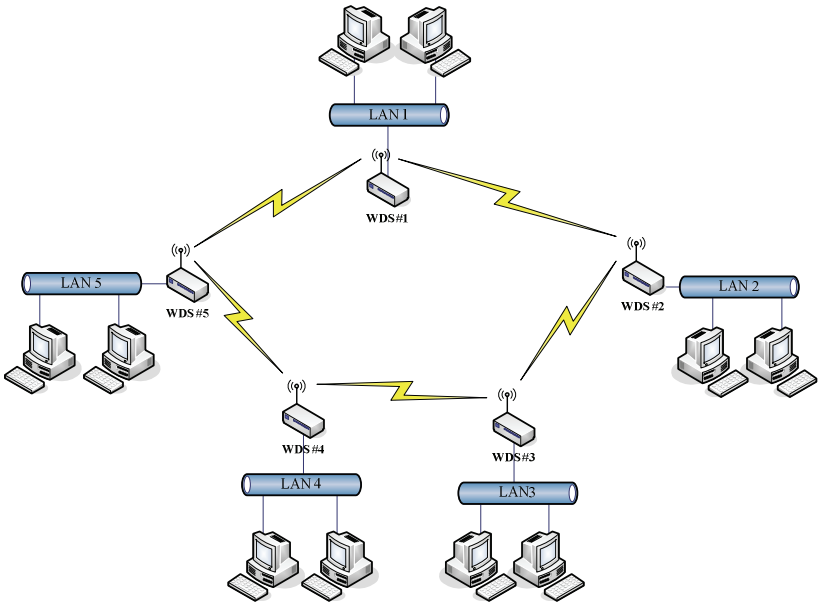
Device	Entries in WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Address of WDS2	No
WDS2	The MAC Addresses of WDS1 and WDS3	No
WDS3	The MAC Addresses of WDS2 and WDS4	No
WDS4	The MAC Addresses of WDS3 and WDS5	No
WDS5	The MAC Address of WDS4	No

Star topology



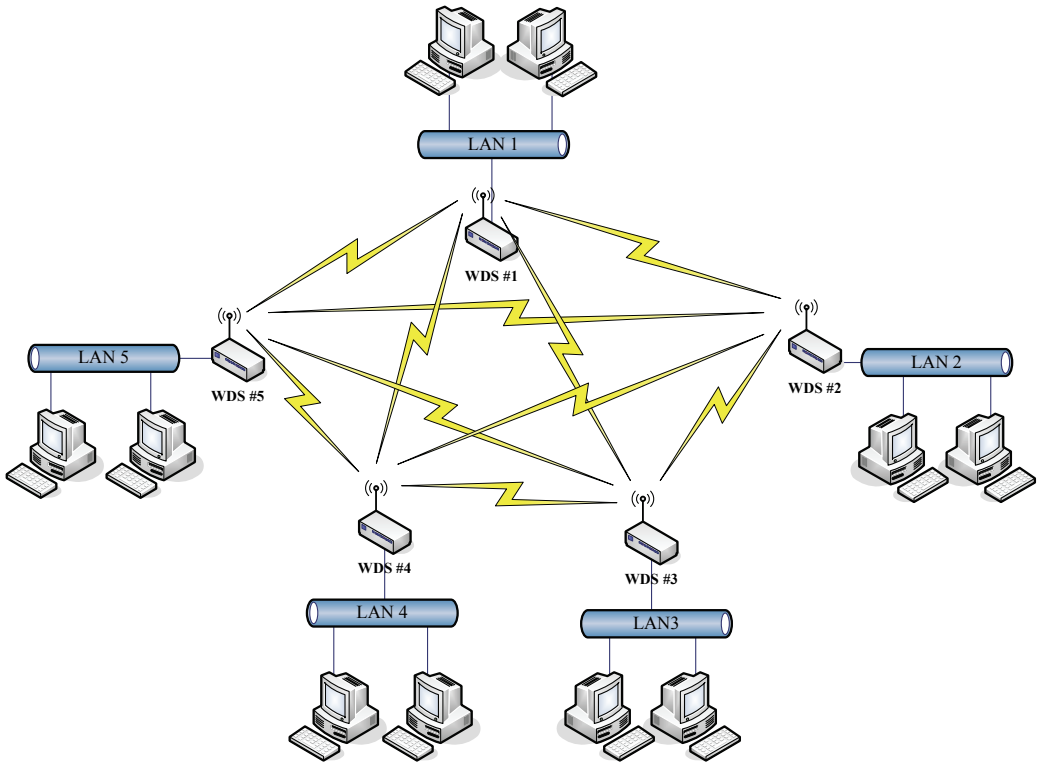
Device	Entries in WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2, WDS3, WDS4 and WDS5	No
WDS2	The MAC Address of WDS1	No
WDS3	The MAC Address of WDS1	No
WDS4	The MAC Address of WDS1	No
WDS5	The MAC Address of WDS1	No

Ring topology



Device	Entries in WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2 and WDS5	Yes
WDS2	The MAC Addresses of WDS1 and WDS3	Yes
WDS3	The MAC Addresses of WDS2 and WDS4	Yes
WDS4	The MAC Addresses of WDS3 and WDS5	Yes
WDS5	The MAC Addresses of WDS4 and WDS1	Yes

Mesh topology



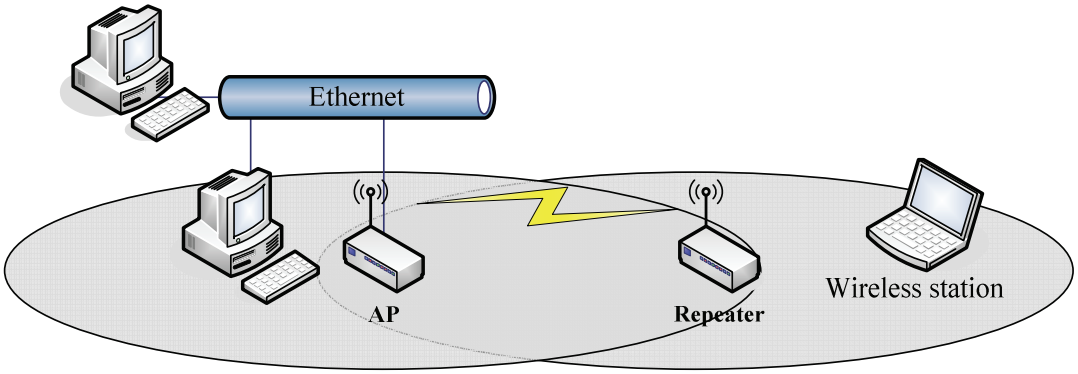
Device	Entries in WDS AP List	Spanning Tree Protocol Required
WDS1	The MAC Addresses of WDS2, WDS3, WDS4 and WDS5	Yes
WDS2	The MAC Addresses of WDS1, WDS3, WDS4 and WDS5	Yes
WDS3	The MAC Addresses of WDS1, WDS2, WDS4 and WDS5	Yes
WDS4	The MAC Addresses of WDS1, WDS2, WDS3 and WDS5	Yes
WDS5	The MAC Addresses of WDS1, WDS2, WDS3 and WDS4	Yes

WDS Application

Wireless Repeater

Wireless Repeater can be used to increase the coverage area of another device (Parent AP). Between the Parent AP and the Wireless Repeater, wireless stations can move among the coverage areas of both devices. If you decide to use WDS as a Repeater, refer the following instructions for configuration.

- The operation mode will normally be Bridge.
- Under Wireless-Basic Settings, select the mode AP+WDS.
- You must select the same radio channel for connected devices, but you may use different SSID.
- Under Wireless-WDS Settings, click **Enable WDS** and enter the MAC address of any remote access point. For any remote access point(s), enter the Repeater's MAC address.
- Change DHCP from **Server** to either **Disabled** or **Client** (unless DHCP Server is required on one of the units). If selecting **Disabled**, make sure to give each AP a different IP address.



Description	Entries of WDS AP List	Spanning Tree Protocol Required
Access Point	The MAC Address of Repeater	Yes
Repeater	The MAC Address of Access Point	Yes

Wireless Bridge

As a Wireless Bridge, the AP-G250 can establish a wireless connection between two or more wired LANs. This is typically used for building-to-building connections. In WDS only mode, no SSID is broadcast and clients can't connect since it is not operating as an access point. This is typically done with directional type antennas pointed towards

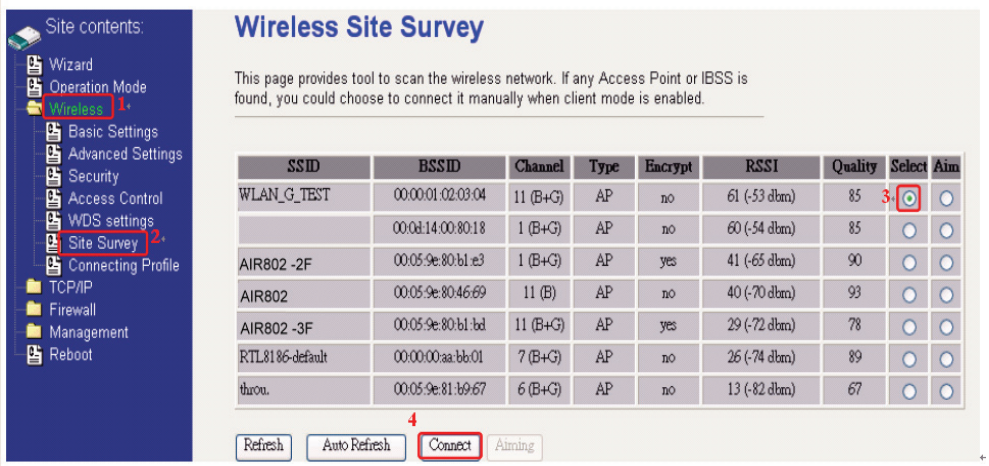
each other. If you decide to use WDS as a Wireless Bridge, refer the following instructions for configuration.

- The operation mode will normally be Bridge in this application.
- Under Wireless-Basic Settings, select the mode WDS.
- Under Wireless-WDS Settings, click **Enable WDS** and enter the MAC address of any remote access point. For any remote access point(s), enter the Repeater's MAC address.
- Change DHCP from **Server** to either **Disabled** or **Client**. If selecting disabled, make sure to give each AP a different IP address so that all units do not have the same IP address.

Site Survey

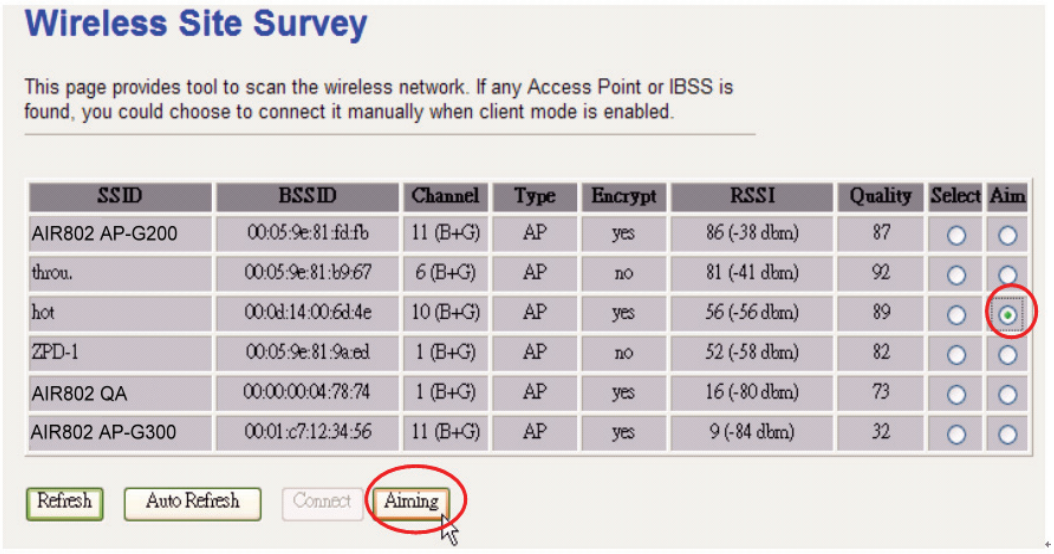
Scanning

This tool allows you to scan for nearby available networks. If Client Mode is enabled, you can choose to manually connect to any Access Point or IBSS found.

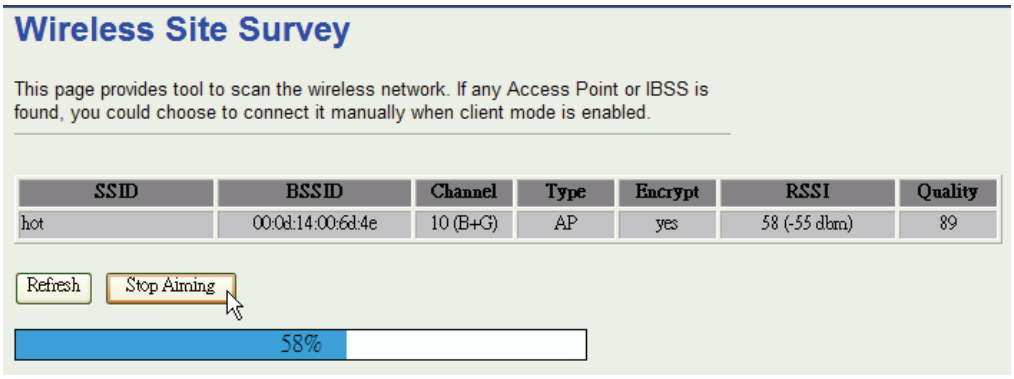


Aiming Tool

The "Aiming Tool" can help the installer of the AP-G250 find the best direction targeting the specific Access Point or IBSS. It displays the RSSI of the specify SSID on the Wireless Site Survey page on the web and LED, so the installer can adjust the antenna and visually check RSSI by LED.


Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.
SSID BSSID Channel Type Encrypt RSSI Quality Select Aim
AIR802 AP-G200 00:05:9e:81:fd:fb 11 (B+G) AP yes 86 (-38 dbm) 87
throu. 00:05:9e:81:b9:67 6 (B+G) AP no 81 (-41 dbm) 92
hot 00:0d:14:00:6d:4e 10 (B+G) AP yes 56 (-56 dbm) 89
ZPD-1 00:05:9e:81:9a:ed 1 (B+G) AP no 52 (-58 dbm) 82
AIR802 QA 00:00:00:04:78:74 1 (B+G) AP yes 16 (-80 dbm) 73
AIR802 AP-G300 00:01:c7:12:34:56 11 (B+G) AP yes 9 (-84 dbm) 32
Refresh
Auto Refresh
Connect
Aiming

When the AP-G250 is in AP Client mode, click the **Aim** option of any SSID on the list in the Wireless Site Survey page and then click the **Aiming** button.

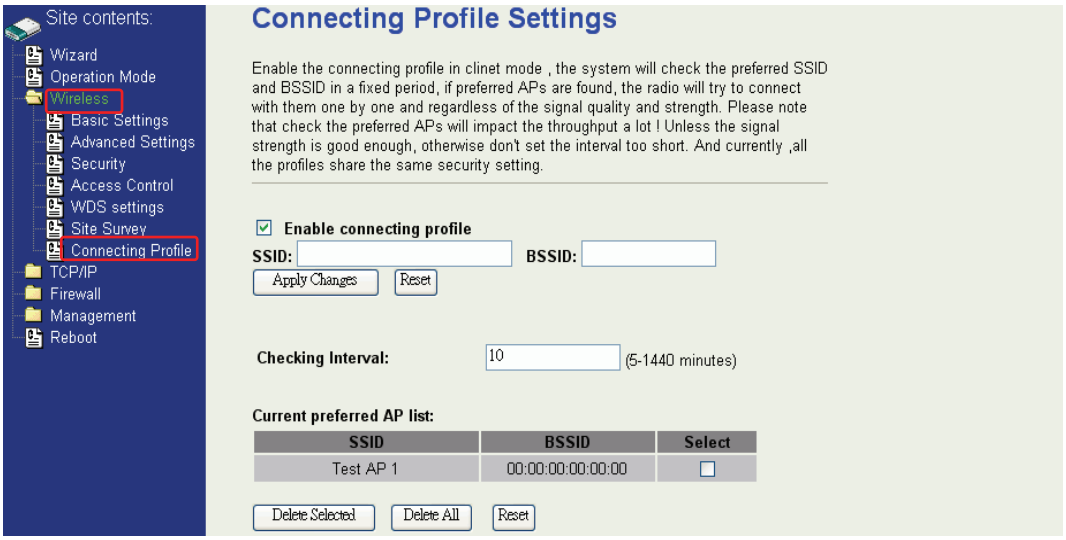

Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.
SSID BSSID Channel Type Encrypt RSSI Quality
hot 00:0d:14:00:6d:4e 10 (B+G) AP yes 58 (-55 dbm) 89
Refresh
Stop Aiming
58%

RSSI is displayed on the web page.

To stop the Aiming tool, click the **Stop Aiming** button.

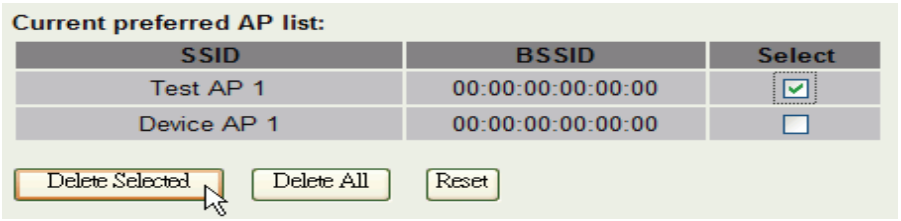
Connecting Profile

To enable this function, this device must be in the client mode. If you are using the AP-G250 as a client device to another access point, this feature will allow you to automatically re-connect to a specific network in the event the link is brought down. Users click to enable this function and type into the SSID field the name of the desired access point and then click Apply Changes.


Site contents:
Wizard
Operation Mode
Wireless
Basic Settings
Advanced Settings
Security
Access Control
WDS settings
Site Survey
Connecting Profile
TCP/IP
Firewall
Management
Reboot
Connecting Profile Settings
Enable the connecting profile in clinet mode , the system will check the preferred SSID and BSSID in a fixed period, if preferred APs are found, the radio will try to connect with them one by one and regardless of the signal quality and strength. Please note that check the preferred APs will impact the throughput a lot ! Unless the signal strength is good enough, otherwise don't set the interval too short. And currently ,all the profiles share the same security setting.
Enable connecting profile
SSID:
BSSID:
Apply Changes
Reset
Checking Interval:
10
(5-1440 minutes)
Current preferred AP list:
SSID
BSSID
Select
Test AP 1
00:00:00:00:00:00
Delete Selected
Delete All
Reset

The BSSID field is an option in case two preferred APs have the same SSID. In this case, this device will check both SSID and BSSID and connect to the matching AP. Normally the BSSID field is left empty.

After enabling the connecting profile, the system checks the preferred SSID in a fixed period (which is set in the Checking Interval in minutes). If preferred APs are found, the radio will try to connect with them one by one from the top to the bottom of the list, regardless of the signal quality and strength. If you have more than one preferred AP, place the most desired at the beginning in order for it to connect first. It should be noted that checking the preferred AP(s) will have an impact on the throughput. If signal strength is not strong, do not set the checking interval too short. The default value is 10 minutes.



To delete an SSID in the list, click the Select box, click **Delete Selected** and then click **OK** in the pop-up window to confirm it. To delete all SSIDs, click Delete All.

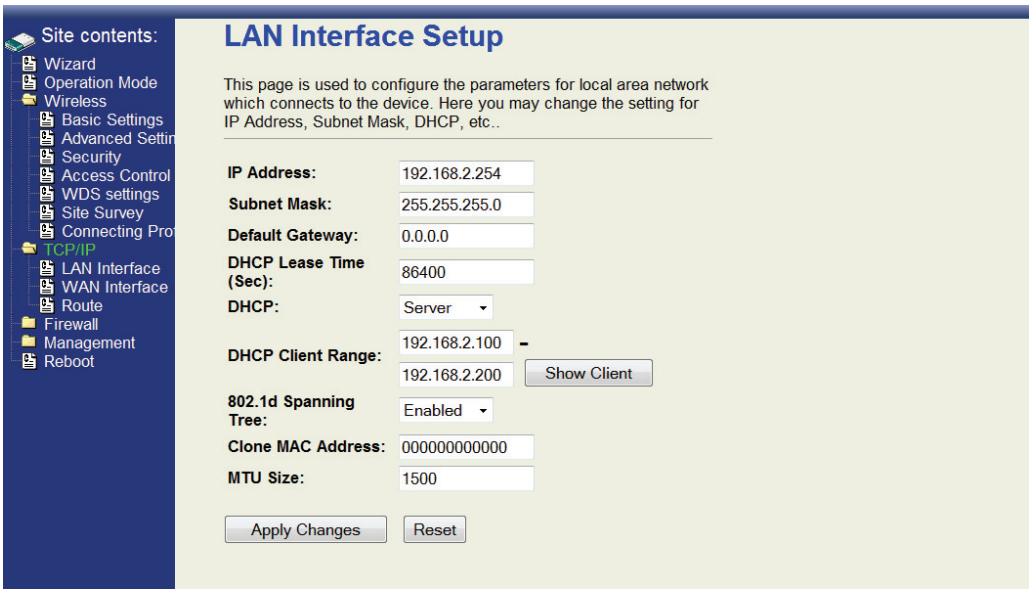
To disable this function, click the check box beside **Enable connecting profile** to remove the check mark. The preferred AP list will be preserved for future use.

TCP/IP CONFIGURATION

LAN Interface

IP Address / Subnet Mask

This where the IP address and subnet mask of the AP-G250 are managed. The default IP address is: 192.168.2.254.



Default Gateway

The default gateway is not used unless you have chosen “Router” as the operation mode.

DHCP Lease Time

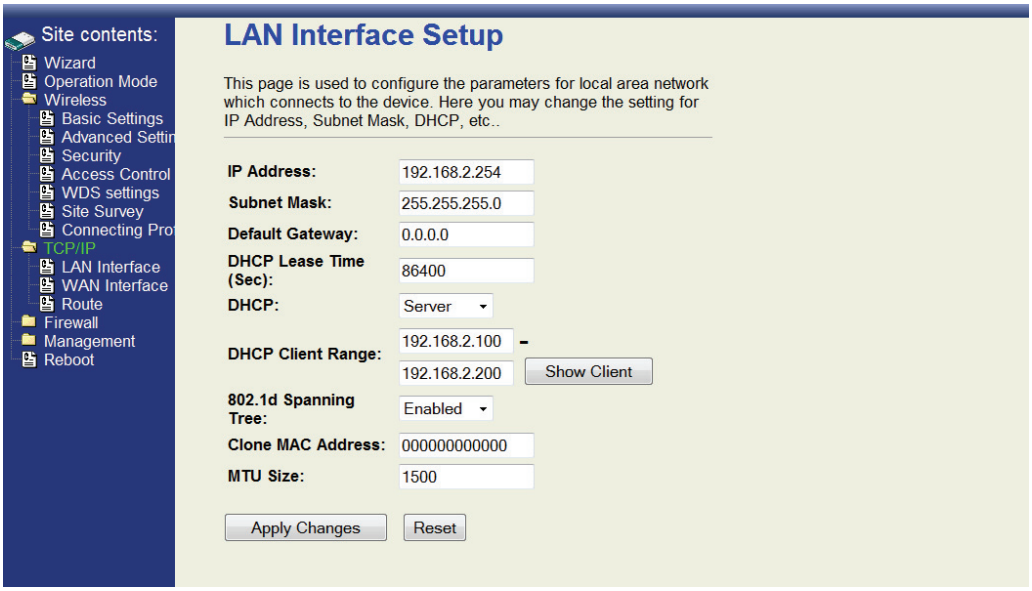
If you have selected the DHCP Server option, the lease time of the IP address held by clients can be defined. This is particularly useful in access points with a high number of daily users.

DHCP Server

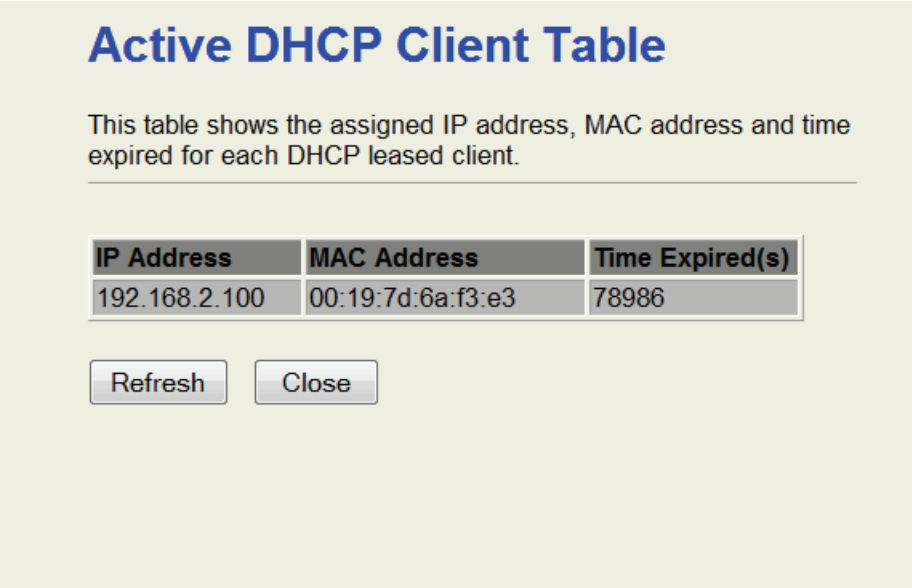
The DHCP options are Server, Client and Disabled. If you use the DHCP server option, make sure that no other DHCP server exists in the same network or you will experience problems. Select **Client** if you want an upstream DHCP server in the network to assign an IP address to manage the AP-G250. Clients will receive their IP address from the upstream server.

DHCP Client Range

Assigns the range or pool of IP addresses that clients receive when the DHCP server option is enabled.



Show Client



802.1d Spanning Tree

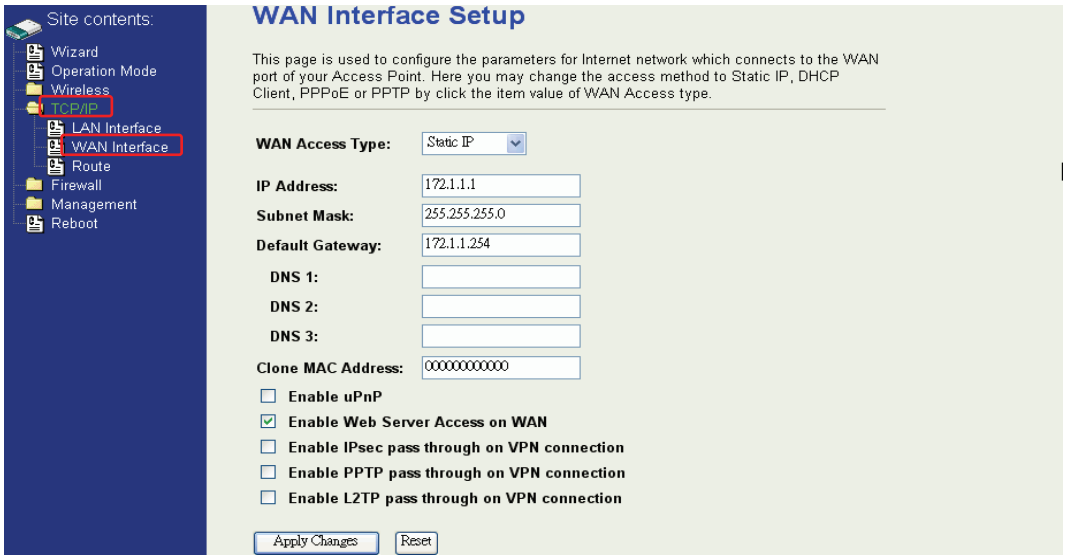
This prevents loops in certain network architectures. It is enabled by default.

WAN Interface

WAN Access Type

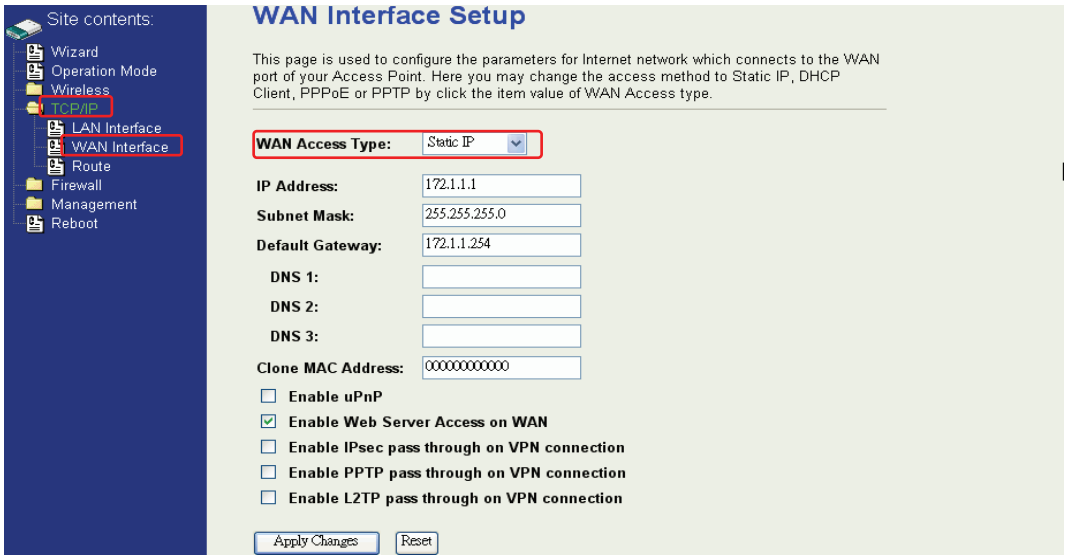
The AP-G250 supports four kinds of IP configuration for the WAN interface: Static IP, DHCP Client, PPPoE and PPTP. Select the appropriate type for your network. The default WAN Access is Static IP. The default IP address of the WAN port is 172.1.1.1.

WAN access type is only applicable in Router or WISP operational modes. If your service provider does not provide a static or “fixed” IP address, then you will likely need to change this to DHCP Client. If using DHCP Client, you can check whether an IP address has been assigned by clicking the Management folder and then the Status page. The current WAN Interface information is located near the bottom of the page.



Static IP

Static or fixed IP addresses are assigned by the network administrator or Internet Service Provider (ISP). If you are using a static IP address, you need to assign these fields: IP address, subnet mask, gateway address, and one of the DNS addresses.



IP Address: The Internet Protocol (IP) address of the WAN interface provided by your ISP or MIS Department.

Subnet Mask: The number used to identify the IP subnet network, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.

Default Gateway: The IP address of the Default Gateway provided by your ISP or MIS Dept. The Default Gateway is the intermediate network device that has knowledge of the network IDs of the other networks in the Wide Area Network, so it can forward the packets to other gateways until they are delivered to the one connected to the specified destination.

DNS 1~3: The IP addresses of the DNS (Domain Name Server) provided by your ISP. DNS is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found. If you select DHCP Client as the WAN access type, you will be presented with the option to “Attain DNS Automatically”. The majority of applications use the automatic option.

Clone MAC Address: Each device on a network has a unique MAC address assigned when manufactured. Certain ISP’s require registration of the MAC address as a security mechanism. However, if you originally registered the MAC address of a computer and later want to add a router, the router MAC address will not be recognized. You can enter the original MAC address from your computer in this field to get around this issue.

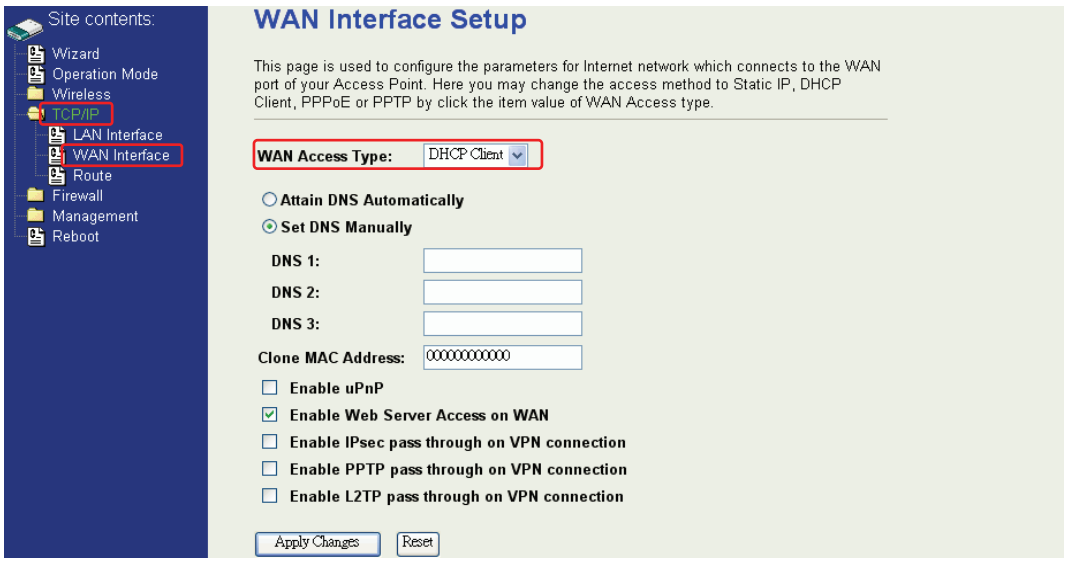
Enable uPnP: This function allows the device to be found and configured automatically by the operating system (e.g., Window XP).

DHCP Client (Dynamic IP)

If you are connecting directly to a cable or DSL modem, particularly in the United States, you are likely getting your IP address dynamically (versus a static or “fixed” IP address). If this is the case, then selecting DHCP Client is the proper choice. Also, if you are connecting the AP-G250 into an existing broadband router (one of the typical four ports) then you will also use DHCP Client.

The AP-G250 gets its IP address from the upstream DHCP server in the network. You can check whether an IP address has been provided to the AP-G250 by clicking the Management folder, then the Status page. WAN Interface information is shown at the bottom of the page. If the IP address is 0.0.0.0, you have not been provided an IP address.

When DHCP-Client WAN Access Type is selected, all IP configuration data besides DNS is from the DHCP server. In many cases, it will be preferable to set the AP-G250 to obtain the DNS automatically. The option “Attain DNS Automatically” appears when DHCP Client is selected as the WAN Type.


Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
LAN Interface
WAN Interface
Route
Firewall
Management
Reboot
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to Static IP, DHCP Client, PPPoE or PPTP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address:
000000000000
Enable uPnP
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
Apply Changes
Reset

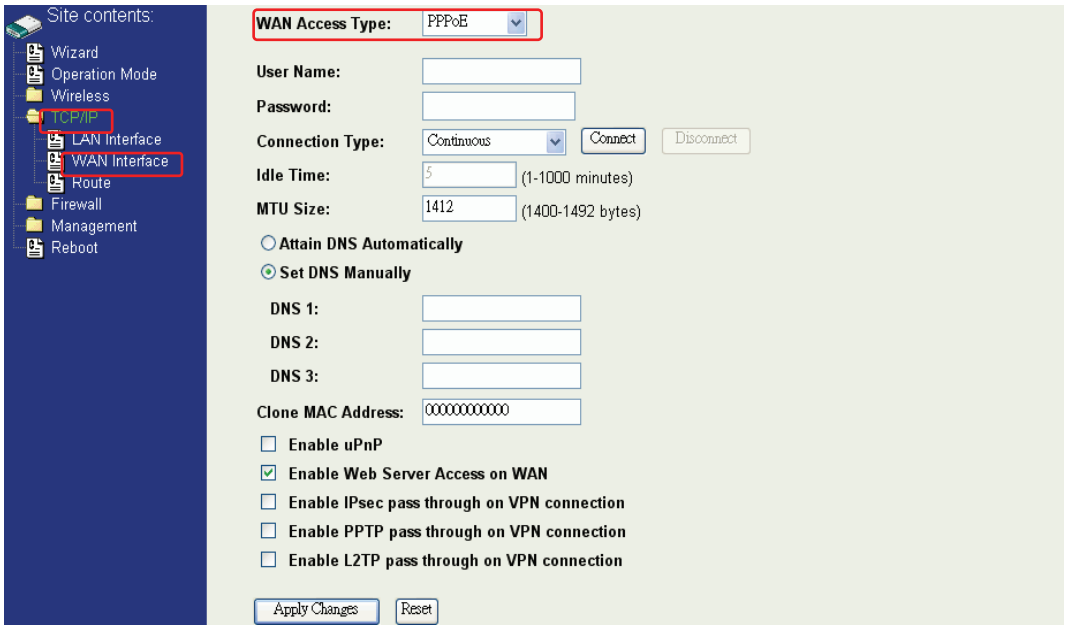
DNS1~3: The IP addresses of the DNS (Domain Name Server) provided by your ISP. DNS is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found. If you select DHCP Client as the WAN access type, you will be presented with the option to “Attain DNS Automatically”. The majority of applications use the automatic option.

Clone MAC Address: Each device on a network has a unique MAC address assigned when manufactured. Certain ISP’s require registration of the MAC address as a security mechanism. However, if you originally registered the MAC address of a computer and later want to add a router, the router MAC address will not be recognized. You can enter the original MAC address from your computer in this field to get around this issue.

Enable uPnP: This function allows the device to be found and configured automatically by the operating system (e.g., Window XP).

PPPoE

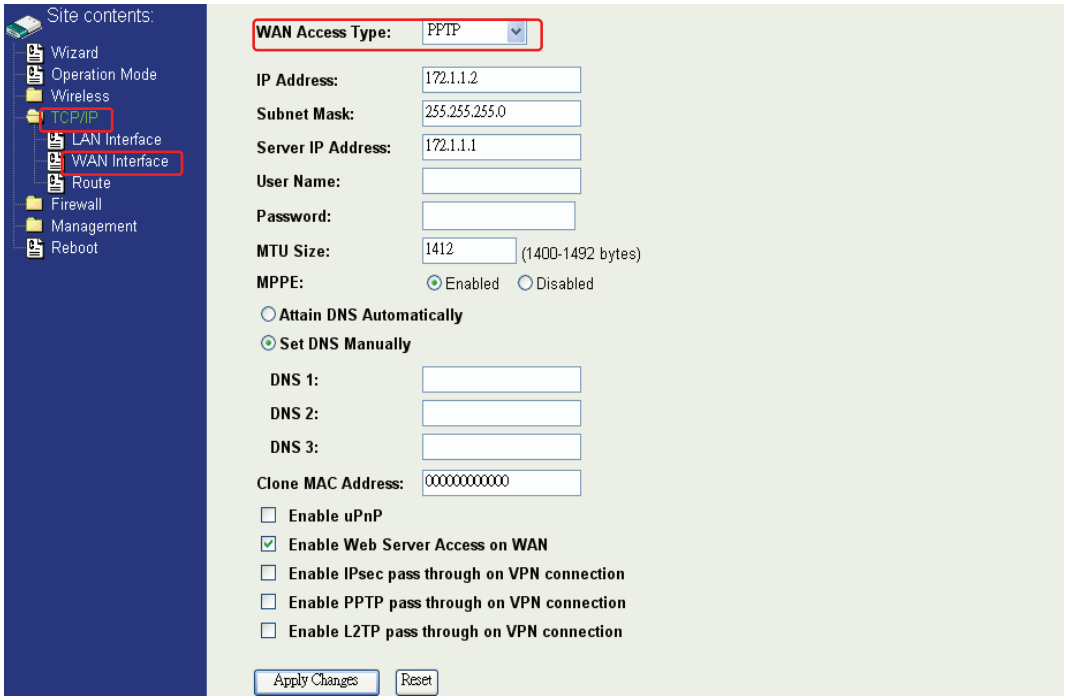
When PPPoE (Point to Point Protocol over Ethernet) WAN Access Type is selected, you must enter the User Name and Password provided by your ISP. The IP configuration is completed when the device successfully authenticates with your ISP.



User Name:	The account provided by your ISP.
Password:	The password for your account.
Connect Type:	Continuous: connect to ISP permanently Manual: Manual connect/disconnect to ISP On-Demand: Automatically connect to ISP when attempting to access the Internet.
Idle Time:	The number of inactive minutes before disconnecting from ISP. This setting is only available when “Connect on Demand” connection type is selected.
MTU Size:	Maximum Transmission Unit. You may need to change the MTU for optimal performance with your specific ISP. The default setting is 1412.
DNS1~3:	The IP addresses of the DNS (Domain Name Server) provided by your ISP. DNS is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.
Clone MAC Address:	Each device on a network has a unique MAC address assigned when manufactured. Certain ISPs require registration of the MAC address as a security mechanism. However, if you originally registered the MAC address of a computer and later want to add a router, the router MAC address will not be recognized. You can enter the original MAC address from your computer in this field to get around this issue.
Enable UPnP:	This function allows the device to be found and configured automatically by the operating system (e.g., Window XP).

PPTP

Point to Point Tunneling Protocol (PPTP) service applies to connections in Europe only.



IP Address: The Internet Protocol (IP) address of the WAN interface provided by your ISP or MIS Department.

Subnet Mask: The number used to identify the IP subnet network, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.

Server IP Address (Default Gateway): The IP address of the PPTP server.

User Name: The account provided by your ISP.

Password: The password of your account.

MTU Size: Maximum Transmission Unit. You may need to change the MTU for optimal performance with your specific ISP. The default setting is 1412.

DNS1~3: The IP addresses of the DNS (Domain Name Server) provided by your ISP. DNS is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.

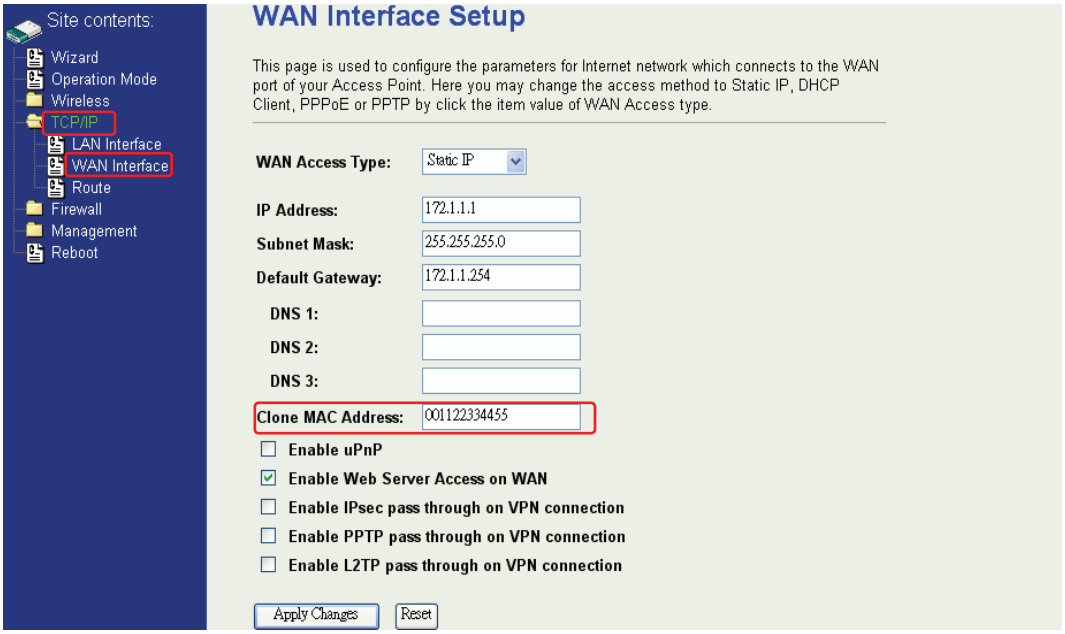
Clone MAC Address: Each device on a network has a unique MAC address assigned when manufactured. Certain ISP's require registration of the MAC address as a security mechanism. However, if you originally registered the MAC address of a computer and later want to add a router, the router MAC address will not be recognized. You can enter the original MAC address from your computer in this field to get around this issue.

Enable uPnP: This function allows the device to be found and configured automatically by the operating system (e.g., Window XP).

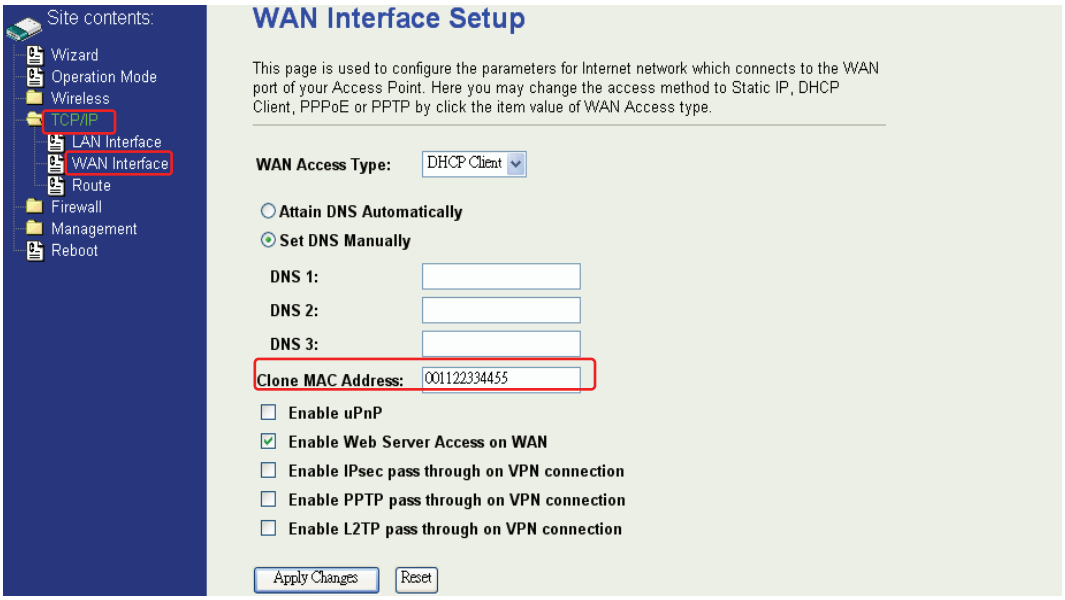
Configuring Clone MAC Address

The AP-G250 provides a MAC address cloning feature to fulfill the requirement of some ISPs that require specification of the client MAC address.

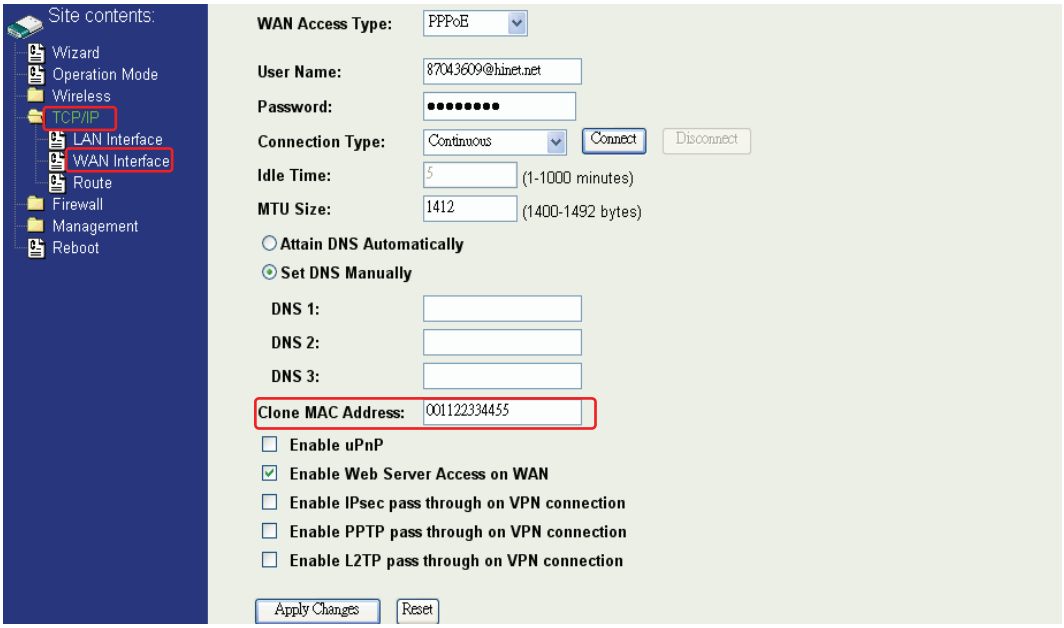
Clone MAC address for Static IP WAN access type:



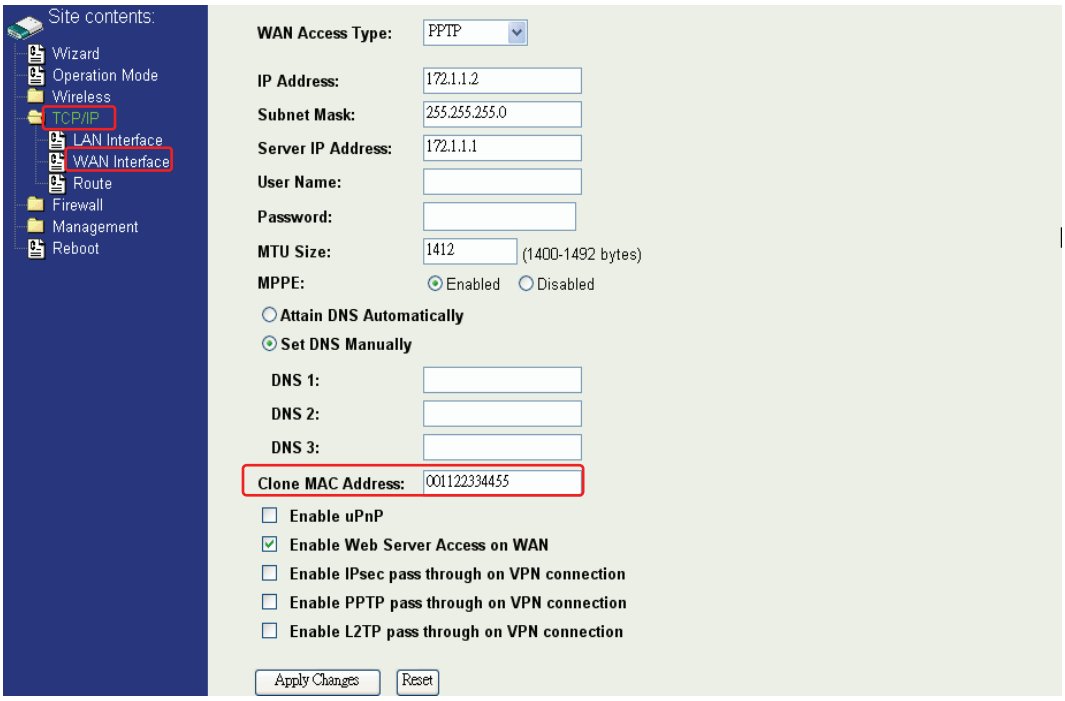
Clone MAC address for DHCP Client WAN access type:


Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
LAN Interface
WAN Interface
Route
Firewall
Management
Reboot
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to Static IP, DHCP Client, PPPoE or PPTP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address:
001122334455
Enable uPnP
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
Apply Changes
Reset

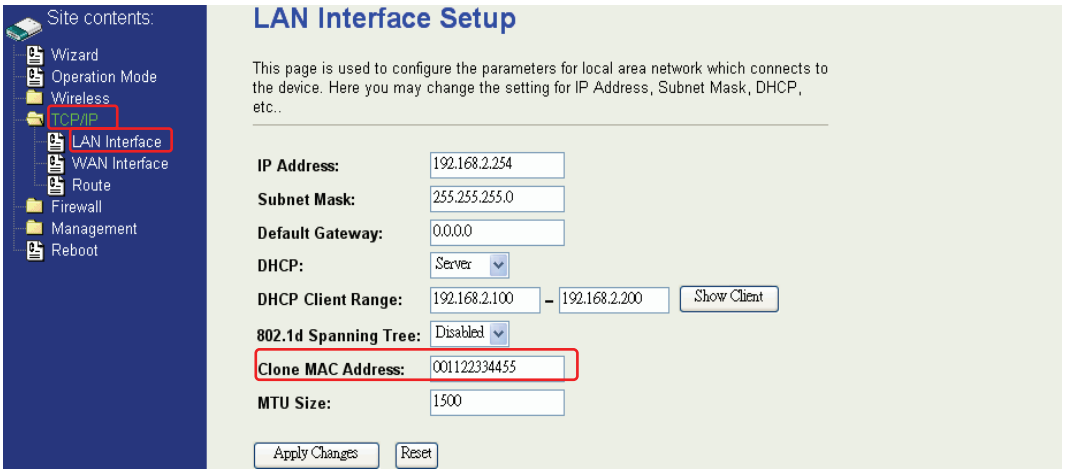
Clone MAC address for PPPoE WAN access type:



Clone MAC address for PPTP WAN access type:

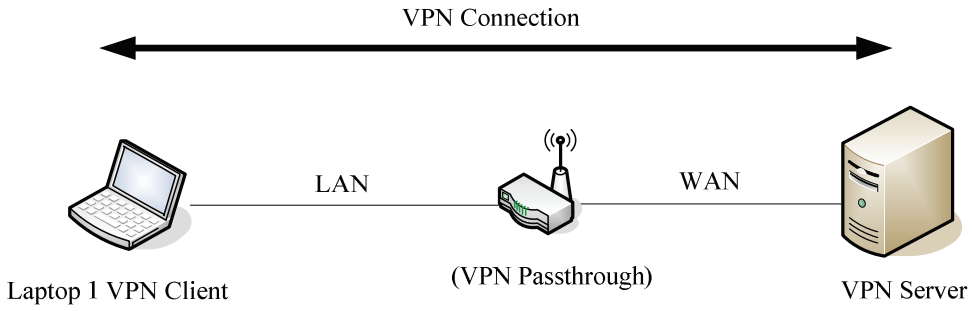


Physical LAN interface MAC address clone:

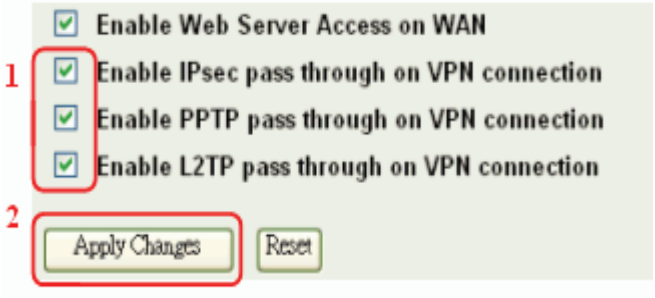


VPN Pass-through

Selection of this option allows Virtual Private Network (VPN) pass-through, including PTP/L2TP/IPsec VPN Connection.

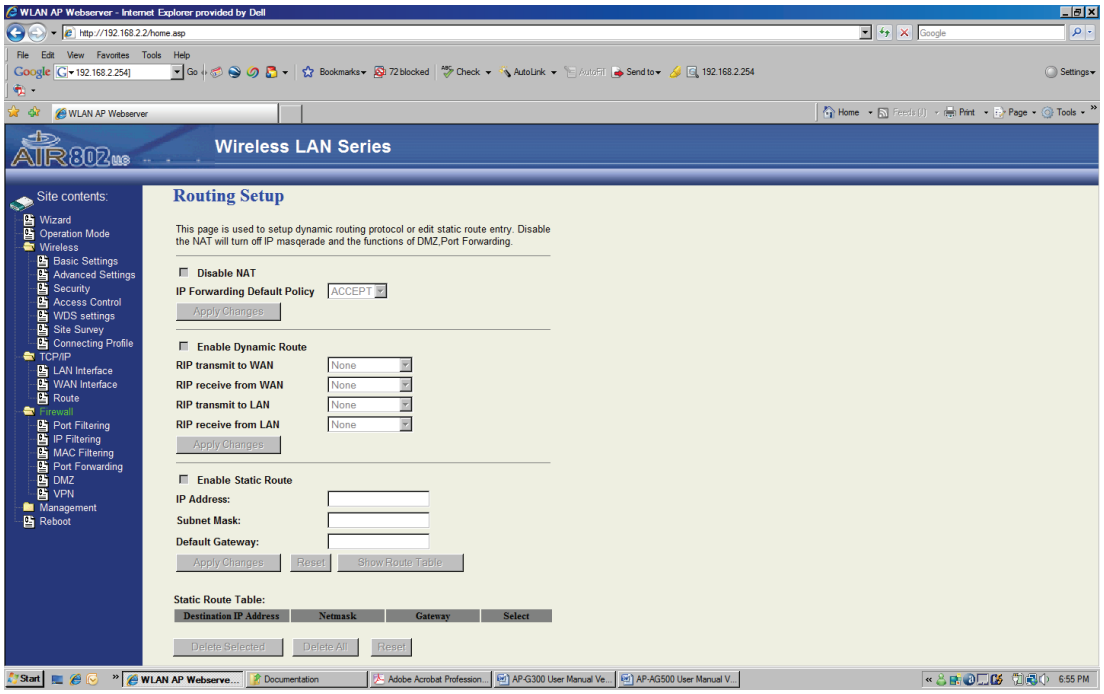


In the WAN Interface section of the TCP/IP Page, check the VPN Pass-through option that you require and click **Apply Changes**.


Enable Web Server Access on WAN
1
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
2
Apply Changes
Reset

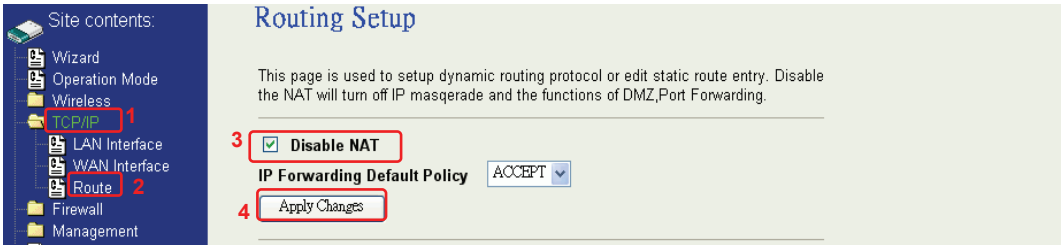
ROUTE

The AP-G250 supports static and dynamic routing. This option is for advanced users and applications.



NAT (Network Address Translation)

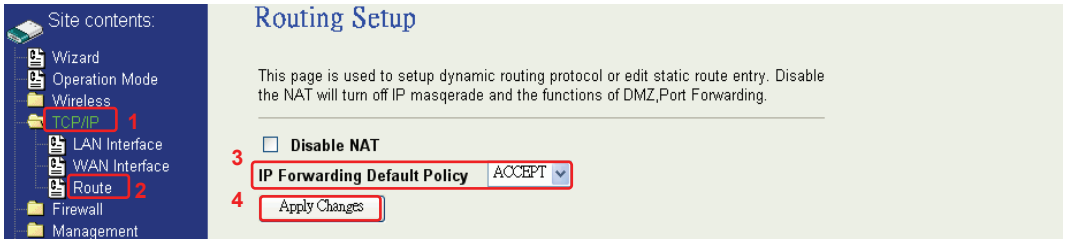
NAT is the translation between public and private IP addresses. When NAT is enabled (under Router or WISP operation modes), you can use port forwarding or DMZ to redirect your common network services. To disable NAT and DMZ functions, go to the TCP/IP-Route page. Port Forwarding will be disabled.



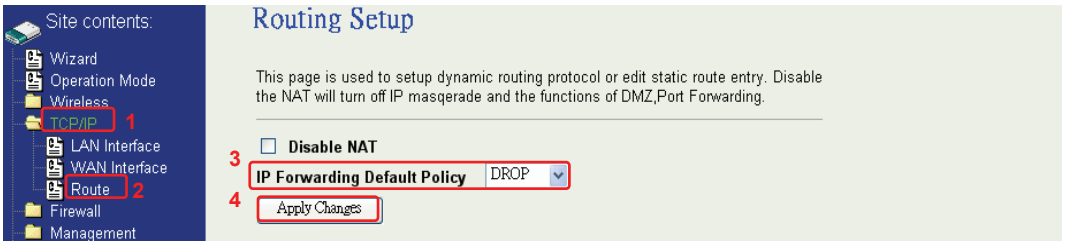
IP Forwarding Default Policy

This option selects whether to Accept or Drop port forwarding. The default is “ACCEPT”.

If you want to block some applications from LAN to WAN, select **ACCEPT** for the IP Forwarding Default Policy.

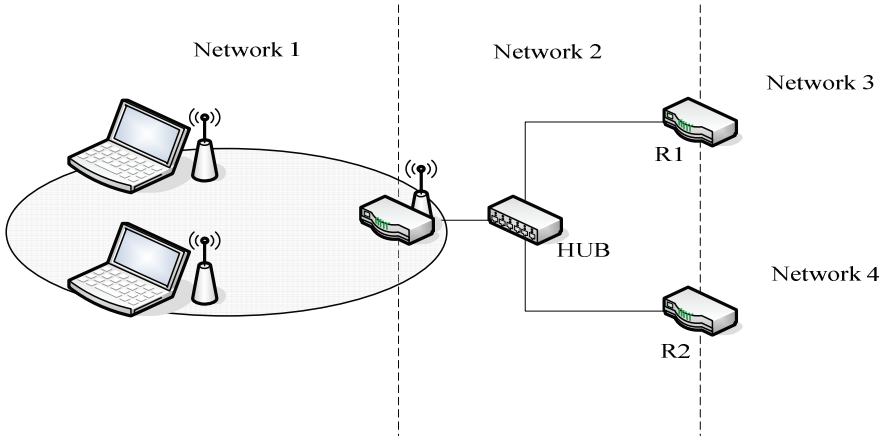


If you want to permit some applications from LAN to WAN, select **DROP**.



Static Route Setup

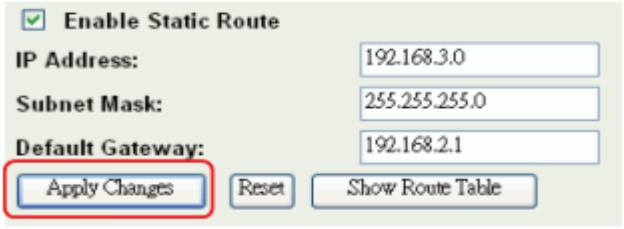
Routes may be statically assigned, if necessary.



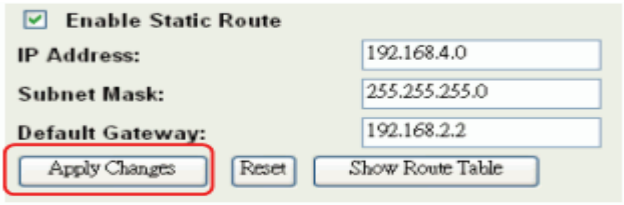
For example, to link Network 3 and Network 4 separately from Network 1, establish a Routing Table configuration as follows:

1. In Route Setup on the TCP/IP page, enable **Static Route**.

2. Enter the IP Address of Network 3, and the Subnet Mask and IP Address of Router R1 in the Default Gateway field.
3. Click **Apply Changes**.



4. Enter the IP Address of Network 4, and the Subnet Mask and the IP Address of Router R2 in the Default Gateway field.
5. Click **Apply Changes**.



6. In the Static Route Table, routes will be shown for Network 3 and Network 4.

Static Route Table:

Destination IP Address	Netmask	Gateway	Select
192.168.3.0	255.255.255.0	192.168.2.1	☐
192.168.4.0	255.255.255.0	192.168.2.2	☐

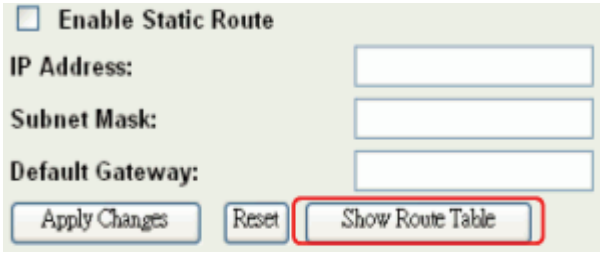
Dynamic Route Setup

Dynamic Routing utilizes RIP 1 and RIP 2 to transmit and receive route information with other routers. To enable dynamic routing:

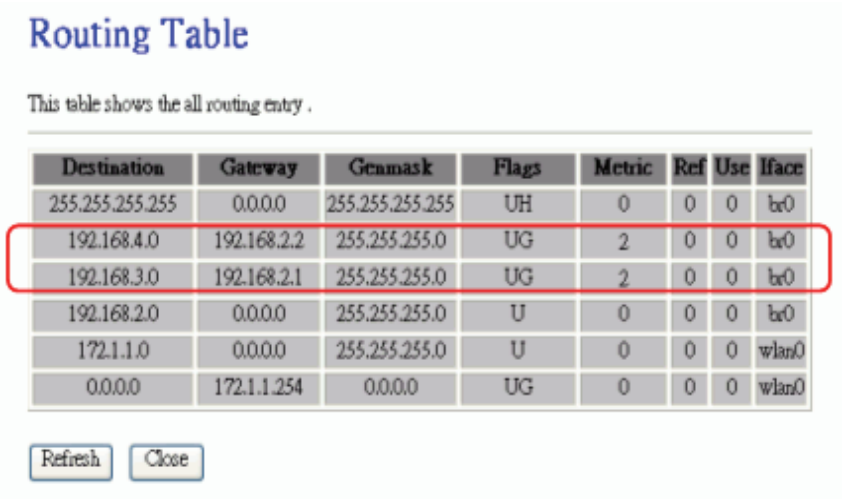
1. In Route Setup, enable **Dynamic Route**.
2. Select RIP 1, RIP 2 or both to transmit/receive packets.

3. Click **Apply Changes**.

4. Click Show Route Table to show the Dynamic Route Table.



5. In the Dynamic Routing Table, routes are shown for Network 3 and Network 4.



FIREWALL CONFIGURATION

Configuring LAN to WAN Firewall

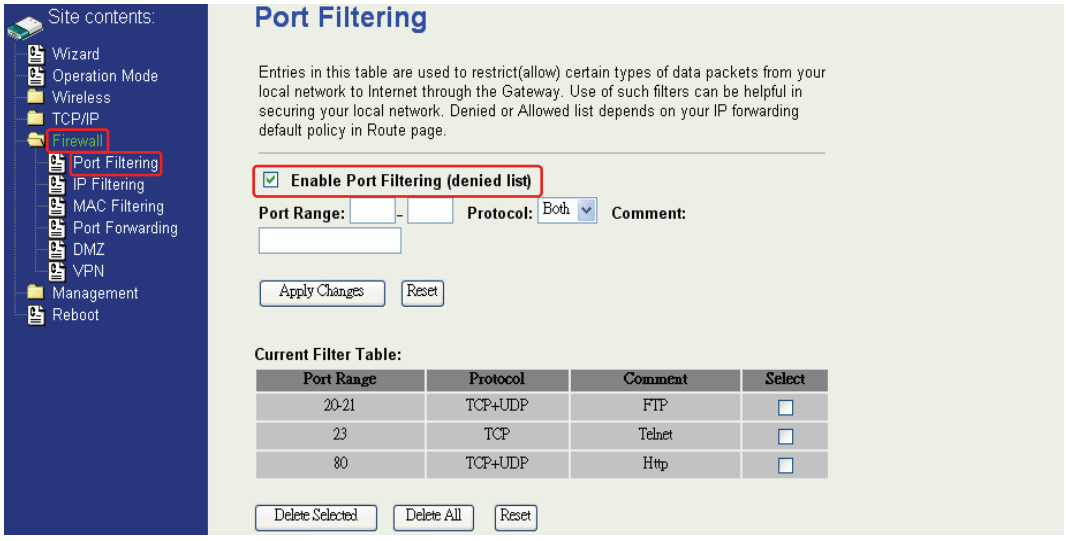
Filtering functions are used to block or permit packets from LAN to WAN. The AP-G250 supports three basic types of filtering.

1. Port Filtering
2. IP Filtering
3. MAC Filtering

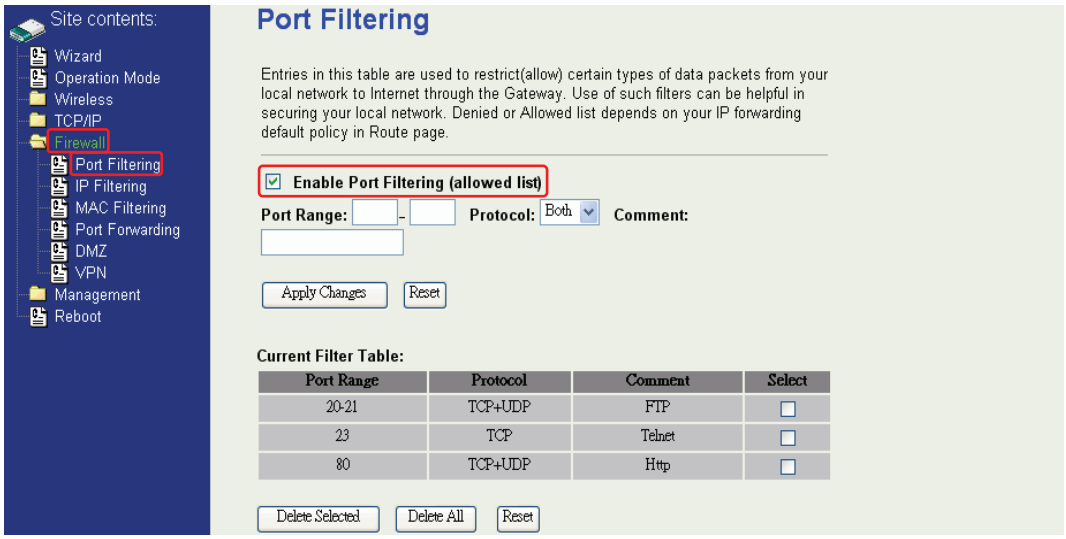
All entries in the current filter table are used to restrict or permit certain types of packets from your local network through the AP-G250. Use of such filters can be helpful in securing or restricting your local network.

Port Filtering

Port forwarding is basically a rule that lets the firewall restrict or allow certain types of data packets from your local area network to the Internet through the Gateway. Once Port Filtering has been enabled, you can define a single port or a range of ports in the Current Filter Table as well as the protocol (TCP, UDP, or Both). The Denied or Allowed list depends upon the IP Forwarding Default Policy defined under the TCP-IP folder and Route. If you select ACCEPT for the IP forwarding default policy (found under TCP/IP, Route), once the source port of outgoing packets match the port definition or within the port ranges in the table, the firewall will block those packets from LAN to WAN.

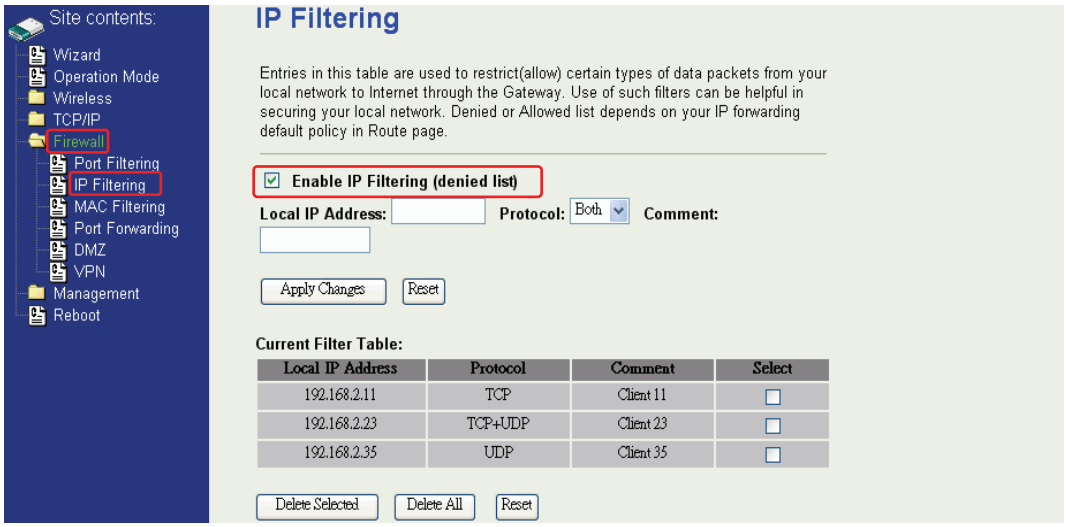


If you select DROP for the IP forwarding default policy, once the source port of outgoing packets match the port definition or are within the port ranges in the table, the firewall will allow those packets form LAN to WAN.

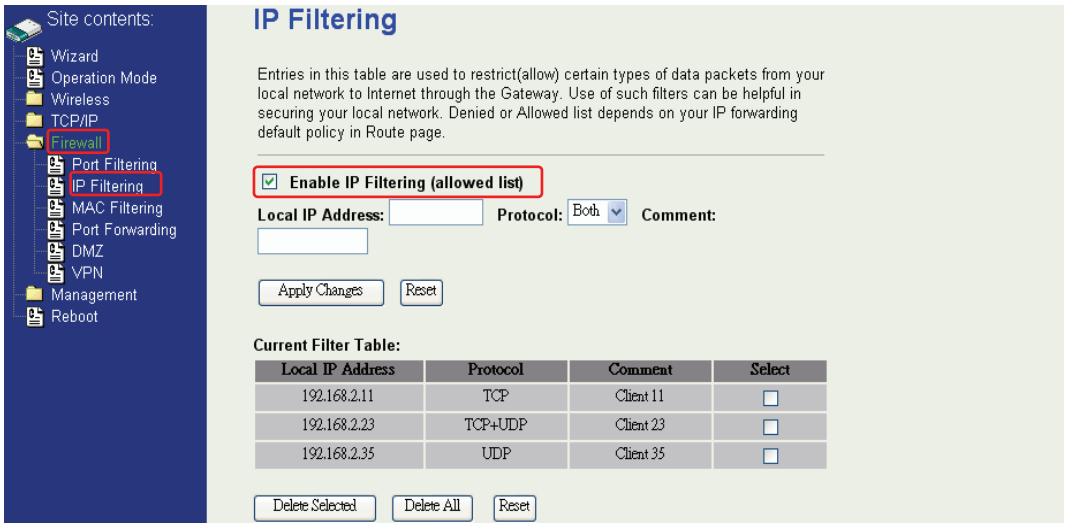

Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Port Filtering
IP Filtering
MAC Filtering
Port Forwarding
DMZ
VPN
Management
Reboot
Port Filtering
Entries in this table are used to restrict(allow) certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing your local network. Denied or Allowed list depends on your IP forwarding default policy in Route page.
Enable Port Filtering (allowed list)
Port Range: - Protocol: Both Comment:
Apply Changes Reset
Current Filter Table:
Port Range Protocol Comment Select
20-21 TCP+UDP FTP
23 TCP Telnet
80 TCP+UDP Http
Delete Selected Delete All Reset

IP Filtering

When you enable the IP Filtering function, you can specify local IP Addresses in the current filter table in addition to specifying TCP, UDP or Both. If you select ACCEPT for the IP forwarding default policy (found under TCP/IP, Route), once the source IP address of outgoing packets match the IP address definition in the table, the firewall will block those packets from LAN to WAN.

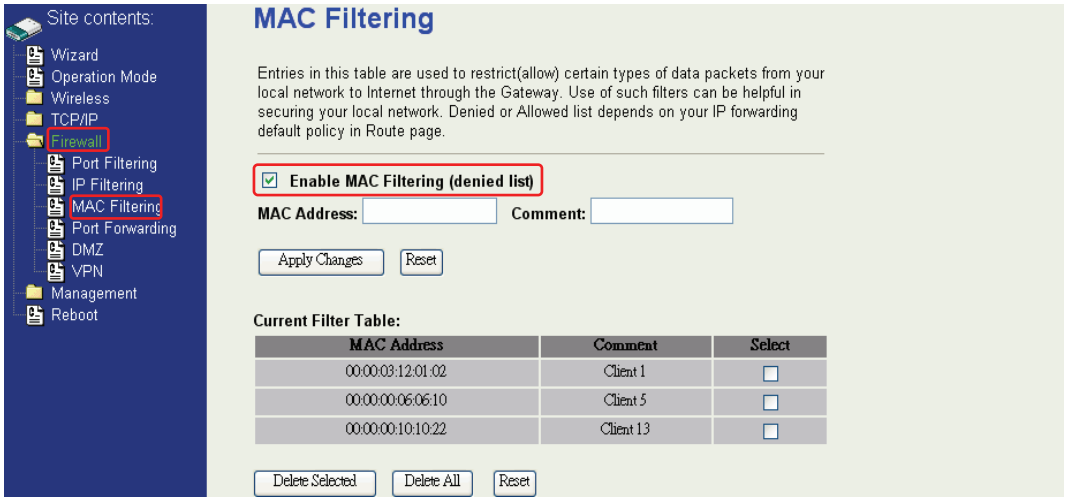

Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Port Filtering
IP Filtering
MAC Filtering
Port Forwarding
DMZ
VPN
Management
Reboot
IP Filtering
Entries in this table are used to restrict(allow) certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing your local network. Denied or Allowed list depends on your IP forwarding default policy in Route page.
Enable IP Filtering (denied list)
Local IP Address: Protocol: Both Comment:
Apply Changes Reset
Current Filter Table:
Local IP Address Protocol Comment Select
192.168.2.11 TCP Client 11
192.168.2.23 TCP+UDP Client 23
192.168.2.35 UDP Client 35
Delete Selected Delete All Reset

If you select DROP for the IP forwarding default policy, once the source IP address of outgoing packets match the IP address definition in the table, the firewall will allow those packets from LAN to WAN.

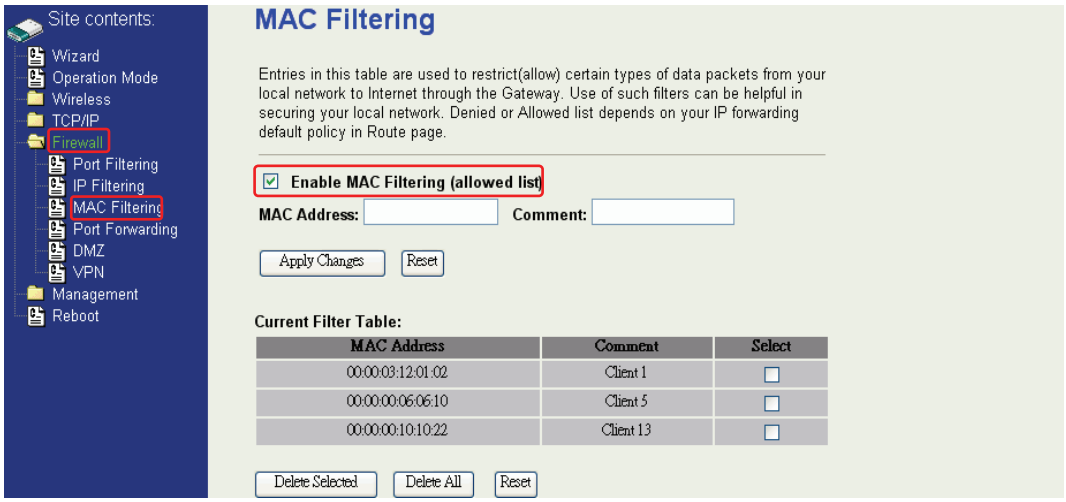


MAC Filtering

When you enable the MAC Filtering function, you can specify the MAC Addresses in the Current Filter Table. If you select ACCEPT for the IP forwarding default policy (found under TCP/IP, then Route), once the source MAC Address of outgoing packets match the MAC Address definition in the table, the firewall will block those packets form LAN to WAN.

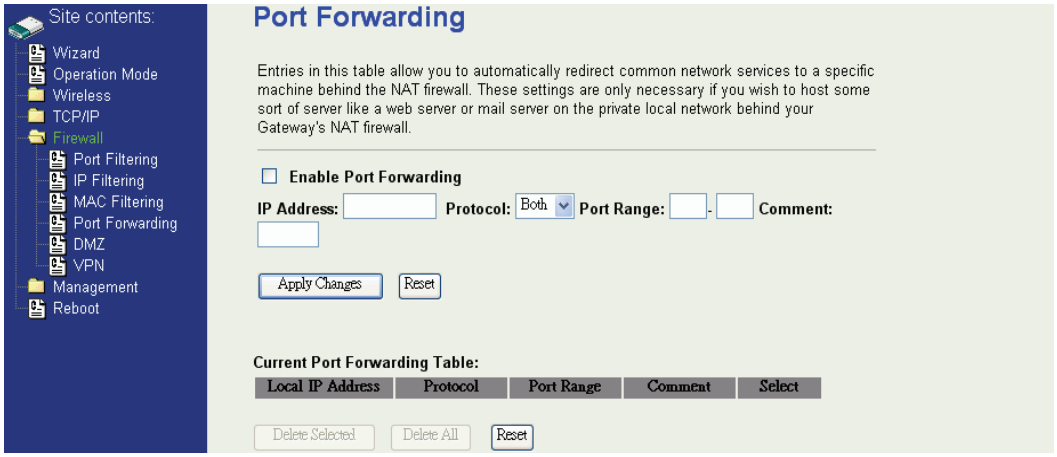


If you select DROP for the IP forwarding default policy, once the source MAC Address of outgoing packets match the MAC Address definition in the table, the firewall will allow those packets form LAN to WAN.



Configuring Port Forwarding (Virtual Server)

This function allows you to automatically redirect common network services to a specific machine behind the AP-G250's NAT firewall. These settings are only necessary if you wish to host some sort of server on the private local network behind NAT firewall, such as a web server or mail server.



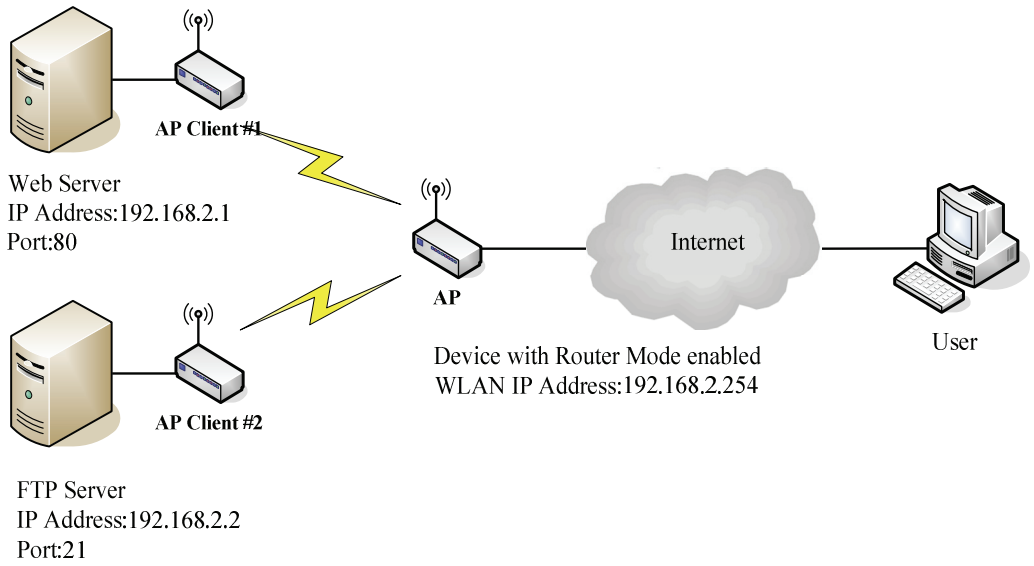
The port numbers used most often are shown in the following table.

Services	Port Number
ECHO	7
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer Protocol)	80
POP3 (Post Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
SIP (Session Initiation Protocol)	5060
PPTP (Point-to-Point Tunneling Protocol)	1723

For other well-know port number assignments, see:
http://www.iana.org/assignments/port-numbers

Multiple Servers behind NAT (Example)

In this case, there are two PCs in the local network accessible for outside users.



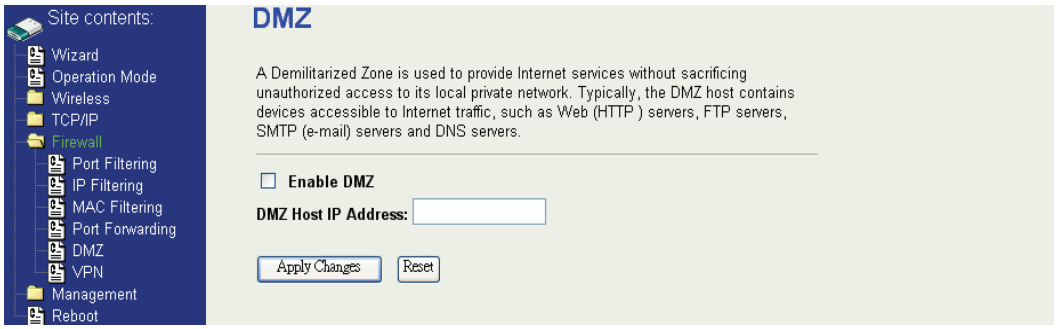
Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
192.168.2.1	TCP+UDP	80	Web Server	☐
192.168.2.2	TCP+UDP	21	FTP Server	☐

Delete Selected | Delete All | Reset

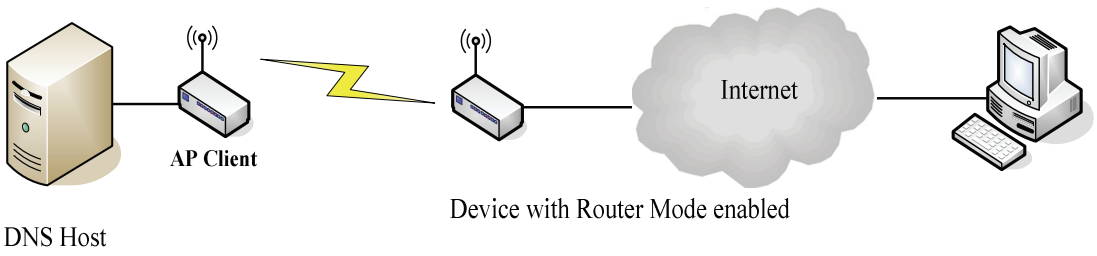
Configuring DMZ

A Demilitarized Zone (DMZ) is used to provide Internet services without sacrificing unauthorized access to the local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. All inbound packets will be redirected to the selected computer. It is also useful when running some applications that use uncertain incoming ports (e.g., Internet games).



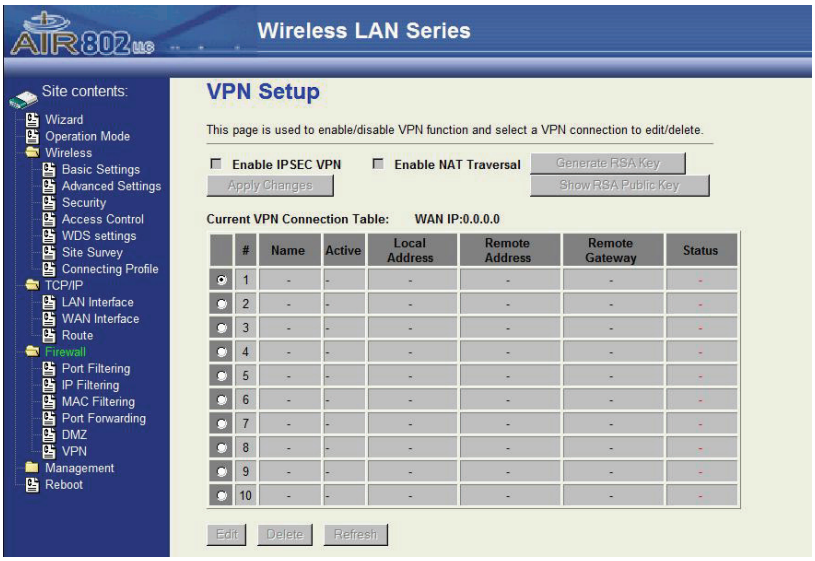
To use a DMZ:

1. Click the check box beside **Enable DMZ**.
2. Enter the IP Address of the computer that you want to expose to Internet in **DMZ Host IP Address**.
3. Click **Apply Changes** to save the changes.



Configuring VPN

The VPN Setup screen provides a means to enable or disable VPN functions and to edit or delete them.



MANAGEMENT

Status

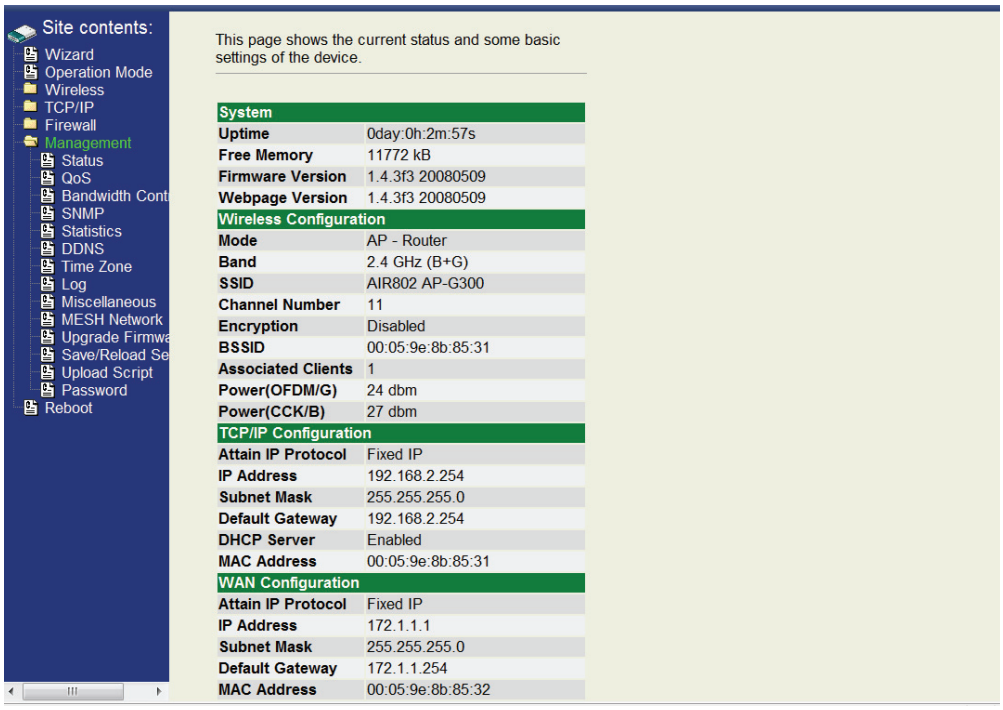
This page provides the current firmware version, system uptime, and status and settings information that can be useful for troubleshooting problems or to see a quick profile of the current configuration.

Depending on the operating mode, the status page also provides two or three other areas of information.

The Wireless Configuration section shows the mode, SSID, channel number, MAC (BSSID) address, number of associated clients and radio power. OFDM represents 802.11g and CCK represents 802.11b.

The TCP/IP Configuration section displays the IP address of the unit, default gateway and the DHCP configuration.

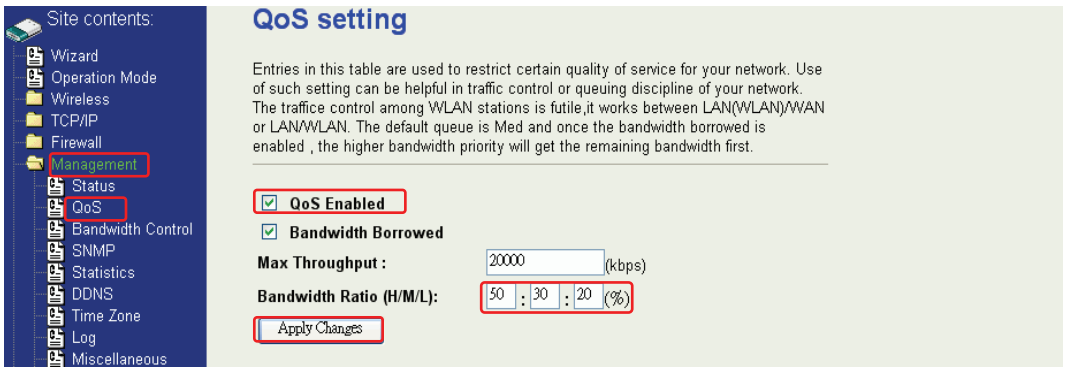
The WAN Configuration section only appears when the AP-G250 is operating in Router or WISP mode. In WISP-Client mode, this is very useful after a connection to another access point is made to see if an IP address has been provided.



Quality of Service (QoS)

Quality of Service (QoS) concerns resource reservation control mechanisms and not the achieved service quality. It is the ability to provide different priority to various applications, users, or data flows, or to guarantee a certain level of performance to a data flow. These guarantees are extremely important in networks with multimedia traffic such as VoIP and video.

AIR802 has implemented some QoS mechanisms in the AP-G250 to allow you to specify some rules to ensure the quality of service in your network. The AP-G250 also provides a Bandwidth Priority function to allocate bandwidth. This function can be helpful in shaping and queuing traffic from LAN (WLAN) to WAN or LAN to WLAN, but not WLAN to WLAN.


Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Status
QoS
Bandwidth Control
SNMP
Statistics
DDNS
Time Zone
Log
Miscellaneous
QoS setting
Entries in this table are used to restrict certain quality of service for your network. Use of such setting can be helpful in traffic control or queuing discipline of your network. The traffice control among WLAN stations is futile,it works between LAN(WLAN)/WAN or LAN/WLAN. The default queue is Med and once the bandwidth borrowed is enabled , the higher bandwidth priority will get the remaining bandwidth first.
QoS Enabled
Bandwidth Borrowed
Max Throughput :
20000
(kbps)
Bandwidth Ratio (H/M/L):
50 : 30 : 20 (%)
Apply Changes

To use QoS:

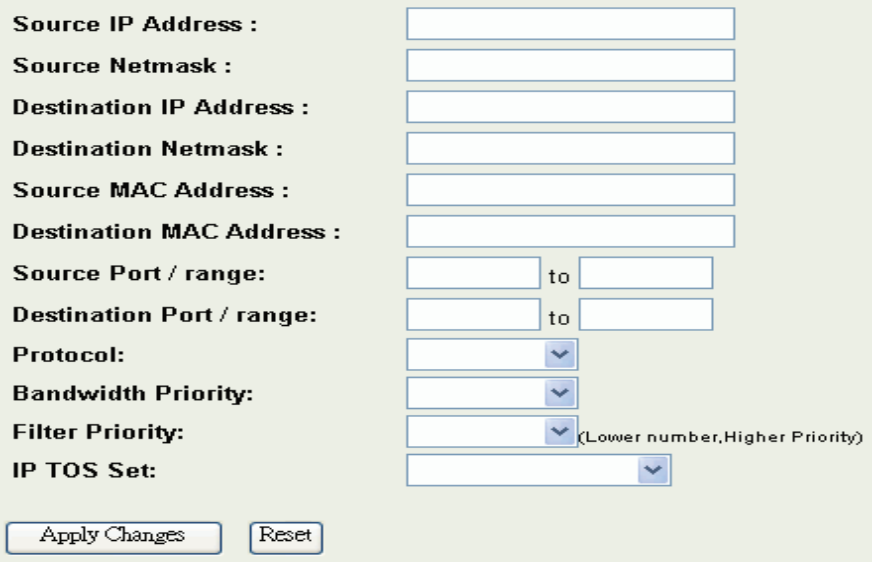
1. Click the **QoS** link under **Management** to open the QoS Setting page.
2. Click the check box beside **QoS Enabled**.
3. Select the **Bandwidth Borrowed** check box if you want to allow a rule to borrow unused bandwidth. Bandwidth borrowing is decided by priority of the rules. Higher priority will get the remaining bandwidth first.
4. Enter the value of Max Throughput that you want to allocate for one rule. The value should between 1200 kbps and 24000 kbps (default is 2000 kbps).
5. Assign the High, Medium and Low Bandwidth Ratios (H/M/L). The following table describes the priorities that you can apply to bandwidth.

Priority Level	Description
High	Typically used for voice or video applications that is especially sensitive to the variations in delay.
Medium	Typically used for important traffic that can tolerate some delay.
Low	Typically used for non-critical traffic such as a large number of transfers but that should not affect other applications.

Range is from 1 to 99, with default priorities: High 50%, Medium 30%, Low 20%.

6. Click **Apply Changes** to save the changes.

QoS Rule Settings



The following table provides more details on the parameters in the above screen.

Label	Description
IP Address	Enter the source and destination IP Address using dotted decimal notation.
Netmask	Enter the source and destination subnet mask address in these fields.
MAC Address	Enter the source and destination MAC Address in these fields.
Port / range	You can enter specific port number or port range of the source and destination.
Protocol	Select a protocol from the drop down list box. Choose TCP/UDP, TCP or UDP.
Bandwidth Priority	Select a bandwidth priority from the drop down list box. Choose Low, Medium or High.
Filter Priority	Select a filter priority number from the drop down list box. Lower number gets higher priority when two rules have the same bandwidth priority.
IP TOS Set	Select an IP type-of-service value from the drop down list box. Choose Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, or Minimize Delay.
Apply Changes	Click this button to save and apply your settings.
Reset	Click this button to begin re-input the parameters.

Current QoS Table of Established Rules

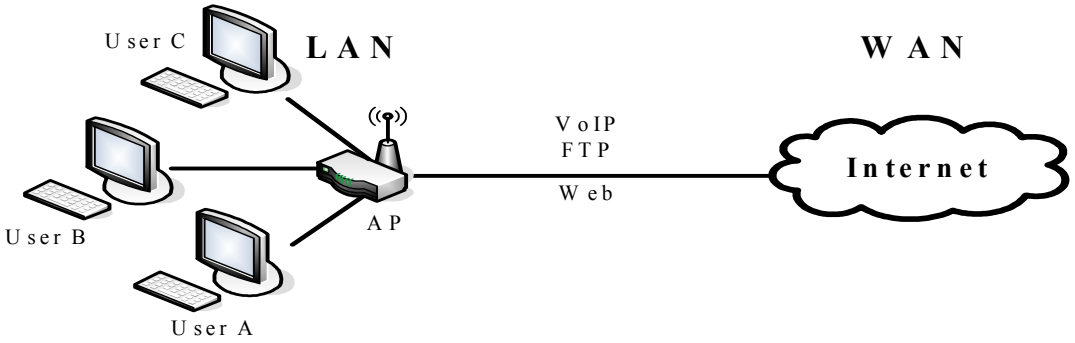
In the Current QoS Setting screen, you can see a list of the rules that have been specified and their associated details. The table can detail 50 rules maximum.

Current QoS Setting:
(Mask 255.255.255.255 means single host)

Src Adr	Dst Adr	Src MAC	Dst MAC	Src Port	Dst Port	Pro	Pri	Filter	TOS	Sel
192.168.2.11/24	140.113.27.181/24	00:05:9e:80:aa:ee	-	21-21	21-21	TCP	LOW	0	Normal	☐
anywhere	anywhere	-	-	80-80	-	TCP/UDP	MED	0	Normal	☐
192.168.2.13/24	anywhere	-	-	50000-50050	-	TCP/UDP	LOW	2	Normal	☐
anywhere	192.168.2.12/24	-	-	-	-	TCP/UDP	MED	1	Normal	☐
192.168.2.15/24	anywhere	00:05:9e:80:aa:cc	-	-	-	TCP/UDP	HIGH	0	Normal	☐

Delete Selected | Delete All | Reset

A Usage Example



There are three users in this network example.

- User A wants to browse websites to retrieve information.
- User B wants to use an FTP connection to download a large file.
- User C wants to use a software IP (VOIP) phone to speak with a customer.

Since VoIP traffic is extremely sensitive to variations in delay, you would set High priority for User C. FTP transmissions can take a long time so you can set Low priority for User B.

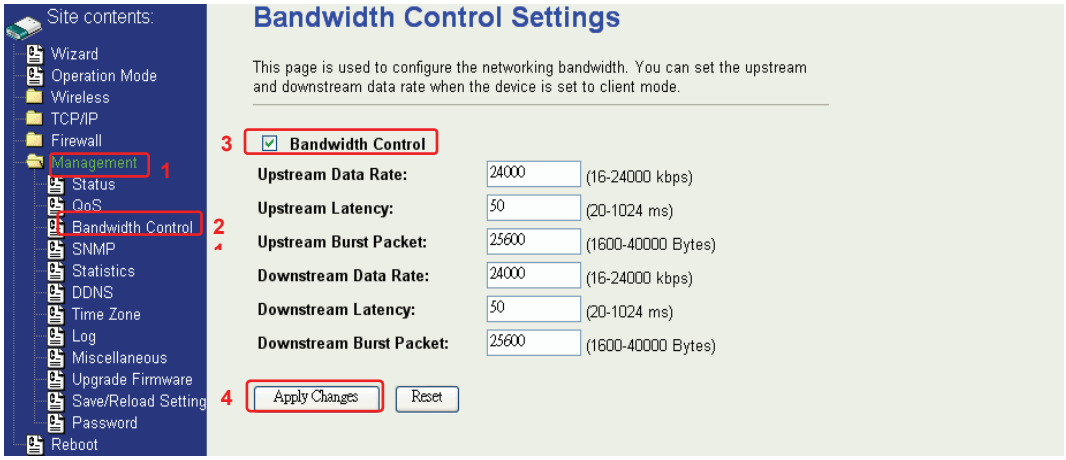
Current QoS Setting:
(Mask 255.255.255.255 means single host)

Src Adr	Dst Adr	Src MAC	Dst MAC	Src Port	Dst Port	Pro	Pri	Filter	TOS	Sel
192.168.2.11/24	anywhere	-	-	5060-5061	-	TCP/UDP	HIGH	0	Normal	☐
192.168.2.12/24	anywhere	-	-	21-21	-	TCP	LOW	0	Normal	☐
192.168.2.13/24	anywhere	-	-	80-80	-	TCP	MED	0	Normal	☐

Delete Selected | Delete All | Reset

Bandwidth Control

This functionality can control downstream and upstream bandwidth when the AP-G250 is in Client or WISP mode. Upstream and downstream are relative to the client site. **Note:** If you are using the AP-G250 as an access point, then bandwidth control is not applicable.



To change Bandwidth Control settings:

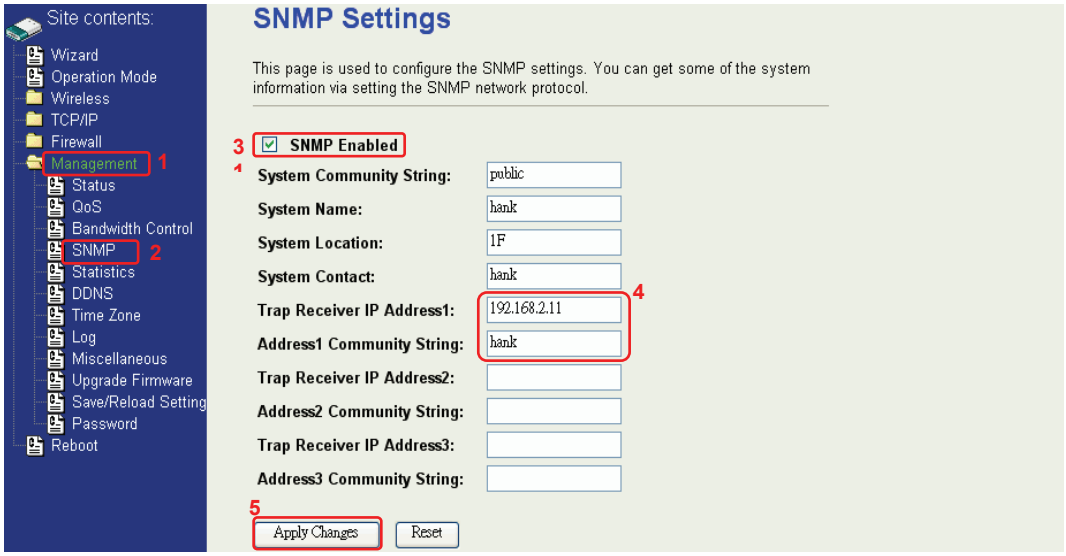
1. Click the **Bandwidth Control** link under **Management** to open the QoS Setting page.
2. Click the check box beside Bandwidth Control.
3. Enter the bandwidth Control parameters.

Parameter	Description
Upstream Data Rate	Speed of data transmission from the Ethernet interface to the wireless interface.
Upstream Latency	The length of time in ms for a data packet to travel from any AIR802 upstream device to your AP-G250 unit.
Upstream Burst Packet	Burst packets are groups consecutive packets with shorter interpacket gaps than packets arriving before or after. Sometimes these come from multiple flows (i.e., data, video). The number of bursts in time (ms) can be defined from the AP-G250 to another AIR802 upstream device.
Downstream Data Rate	Speed of transmit data from Wireless to Ethernet interface.
Downstream Latency	The length of time in ms for a data packet to travel back to your AP-G250 from any AIR802 upstream device.
Downstream Burst Packet	The number of bursts in time (ms) can be defined to the AP-G250 from another AIR802 upstream device.

4. Click **Apply Changes** to save the changes.

SNMP Agent

The AP_G250 is compatible with SNMP v1/v2c and provides standard MIB II. Currently only the “public” community string is available and settings modified by SNMP SET request will be lost after rebooting the device.



To change Bandwidth Control settings:

1. Click the **SNMP** link under **Management** to open the SNMP Settings page.
2. Click the check box beside SNMP Enabled.
3. Enter the SNMP Configuration parameters.

Parameter	Description
System Community String	This is the password sent with each trap to the SNMP Manager.
System Name	Type the name of the device.
System Location	Type the location of the device.
System Contact	Type the name of the person or group to be contacted if the device has problems.
Trap Receiver IP Address	Type the IP Address of the SNMP Manager.
Trap Receiver Community String	This is the password received with trap from the device (SNMP Agent).

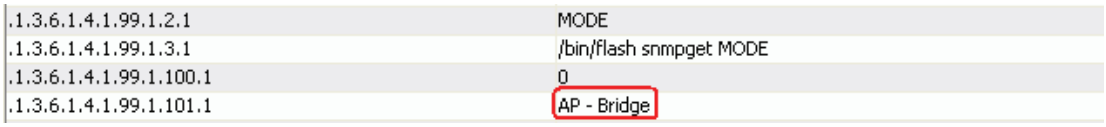
SNMP Traps

Traps	Description
coldStart(0)	The trap from device after reboot the device
linkDown(2)	The trap sent when any of the links are down. See the following table.
linkup(3)	The trap sent when any of the links are up. See the following table.
authenticationFailure(4)	The trap sent when the device receives or sets requirements with the wrong community.

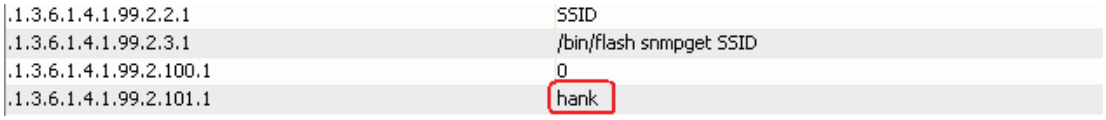
5. Private MIBs

OID	Description
1.3.6.1.4.1.99.1	Operating mode.
1.3.6.1.4.1.99.2	SSID of the device.
1.3.6.1.4.1.99.3	Channel of the device WLAN.
1.3.6.1.4.1.99.4	Band (802.11g / 802.11b only)
1.3.6.1.4.1.99.5	RSSI (Receive Signal Strength Index).
1.3.6.1.4.1.99.6	Active_Clients. The number of associate clients.
1.3.6.1.4.1.99.7	Active_Clients_List. Client's information (MAC Address, Data Rate, RSSI, etc.)
1.3.6.1.4.1.99.8	Type of wireless encryption used.

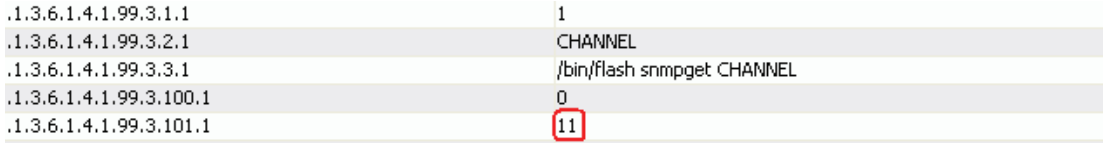
1.3.6.1.4.1.99.1 - Mode



1.3.6.1.4.1.99.2 - SSID



1.3.6.1.4.1.99.3 - Channel



1.3.6.1.4.1.99.4 - Band

.1.3.6.1.4.1.99.4.2.1	BAND
.1.3.6.1.4.1.99.4.3.1	/bin/flash snmpget BAND
.1.3.6.1.4.1.99.4.100.1	0
.1.3.6.1.4.1.99.4.101.1	802.11bg

1.3.6.1.4.1.99.5 - RSSI

.1.3.6.1.4.1.99.5.2.1	RSSI
.1.3.6.1.4.1.99.5.3.1	/bin/flash snmpget RSSI
.1.3.6.1.4.1.99.5.100.1	0
.1.3.6.1.4.1.99.5.101.1	100

1.3.6.1.4.1.99.6 - Active_Clients

.1.3.6.1.4.1.99.6.2.1	ACTIVE_CLIENTS
.1.3.6.1.4.1.99.6.3.1	/bin/flash snmpget ACTIVE_CLIENTS
.1.3.6.1.4.1.99.6.100.1	0
.1.3.6.1.4.1.99.6.101.1	1

1.3.6.1.4.1.99.7 - Active_Clients_List

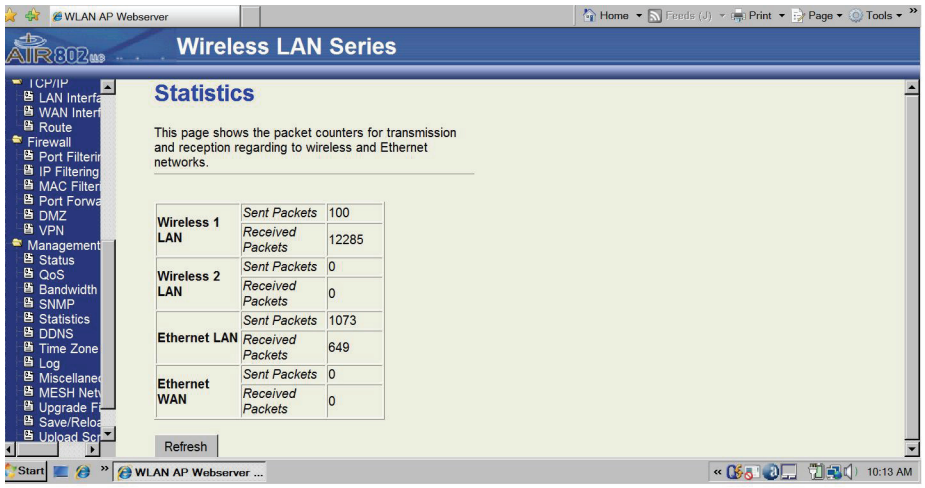
.1.3.6.1.4.1.99.7.2.1	ACTIVE_CLIENTS_LIST
.1.3.6.1.4.1.99.7.3.1	/bin/flash snmpget ACTIVE_CLIENTS_LIST
.1.3.6.1.4.1.99.7.100.1	0 MAC Data Rate RSSI
.1.3.6.1.4.1.99.7.101.1	00:13:02:03:51:5e,102,125,54,no,300,57(-55 dbm)

1.3.6.1.4.1.99.8 - Encryption

.1.3.6.1.4.1.99.8.2.1	ENCRYPTION
.1.3.6.1.4.1.99.8.3.1	/bin/flash snmpget ENCRYPTION
.1.3.6.1.4.1.99.8.100.1	0 AP-WEP
.1.3.6.1.4.1.99.8.101.1	WEP(AP),Disabled(WDS)

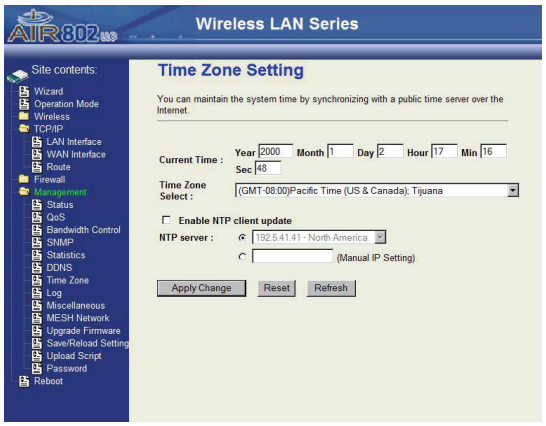
Statistics

Useful information regarding the number of packets sent and received for all interfaces.



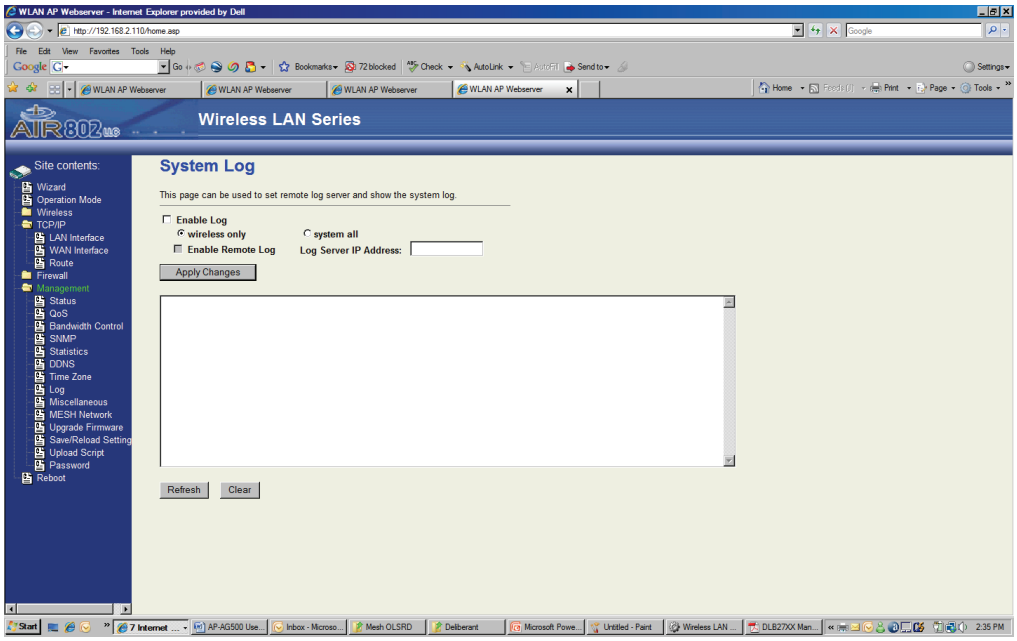
Time Zone Setting

This is used to setup time and to enable NTP client updates for synchronization with a public time server.

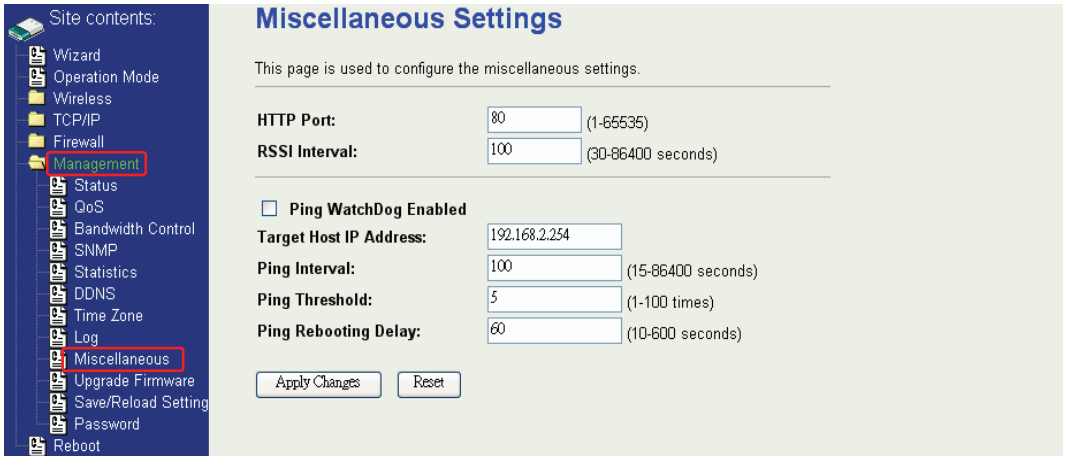

Wireless LAN Series
Site contents:
Time Zone Setting
You can maintain the system time by synchronizing with a public time server over the Internet.
Current Time :
Year 2000 Month 1 Day 2 Hour 17 Min 16
Sec 48
Time Zone Select :
(GMT-08:00)Pacific Time (US & Canada); Tijuana
Enable NTP client update
NTP server :
192.5.41.41 - North America
(Manual IP Setting)
Apply Change
Reset
Refresh

Log

This is used to enable system logs.



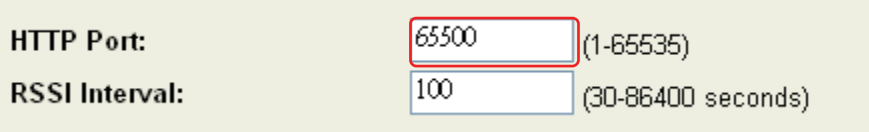
Miscellaneous Settings



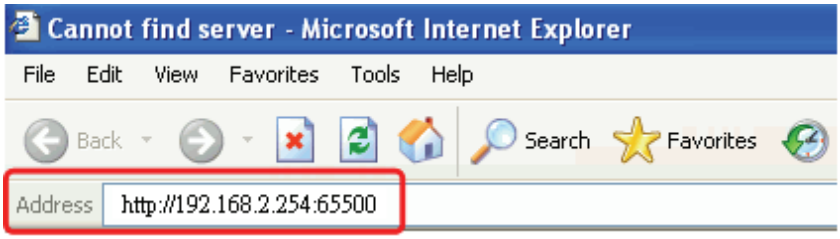
HTTP Port

The default http port is 80. For security concerns, you can change the device's http port to protect this web server from intrusion and attack.

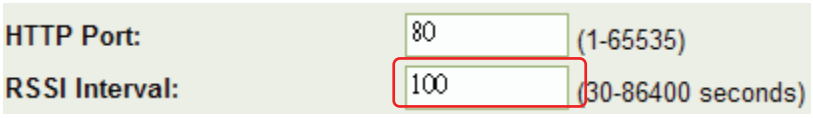
1. Enter the port number you want to change in the HTTP PORT field.



2. Click **Apply Changes**.
3. After applying the change, you should re-login the web server. Type http://192.168.2.254:65500/ in the URL field.



You can also change the RSSI Interval, which specifies the refresh time for RSSI information. The default interval is 100 seconds. Because it has to wait to receive the radio signal, the throughput of this device will be impacted if the interval is too short. The RSSI information can be found on the pages for Wireless Basic Setting, Active Client Table, Wireless Site Survey and Status.



Ping WatchDog

Ping Watchdog is dedicated for continuous monitoring of the connection to the remote host using the Ping tool. Ping works by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. If the defined number of replies is not received, the tool reboots the access point.

The following table lists the Ping WatchDog configuration parameters.

Label	Description
Target Host IP Address	Specifies the IP Address of the target host that will be monitored by Ping Watchdog Tool.
Ping Interval	Specifies the time interval (in seconds) between the ICMP “echo requests” sent by the Ping Watchdog Tool. The default value is 100.
Ping Threshold	Specifies the number of continuous Ping failures before rebooting the access point. The default value is 5.
Ping Rebooting Delay	The time delay before starting the reboot process when the Ping Threshold is met. The default value is 60.

Mesh Network

AIR802 has added a form of mesh networking using Optimized Link State Routing Protocol (OLSR) to the AP-G250. OLSR is a routing protocol for mobile ad-hoc networks that is completely compliant with RFC3626. OLSR is commonly used in community-driven free wireless networks all across the world.

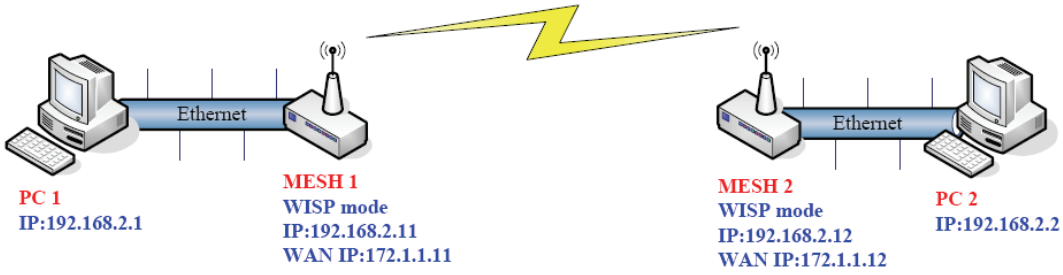
The key concept used in the protocol is multipoint relays (MPRs). MPRs are selected nodes that forward broadcast messages during the flooding process. The protocol is particularly suitable for large and dense networks.

OLSR mesh functions in ad-hoc mode (versus infrastructure mode). It can be used to construct a network for IP video camera surveillance, where both the access points and cameras use static IP address. Up to 30 access points can be connected together in a mesh network. Routing links can be constructed to an external router.

There are two examples shown below. Example 1 represents the basic setup procedures. Example 2 depicts a three-node network for IP video camera surveillance.

EXAMPLE 1

Setup topology



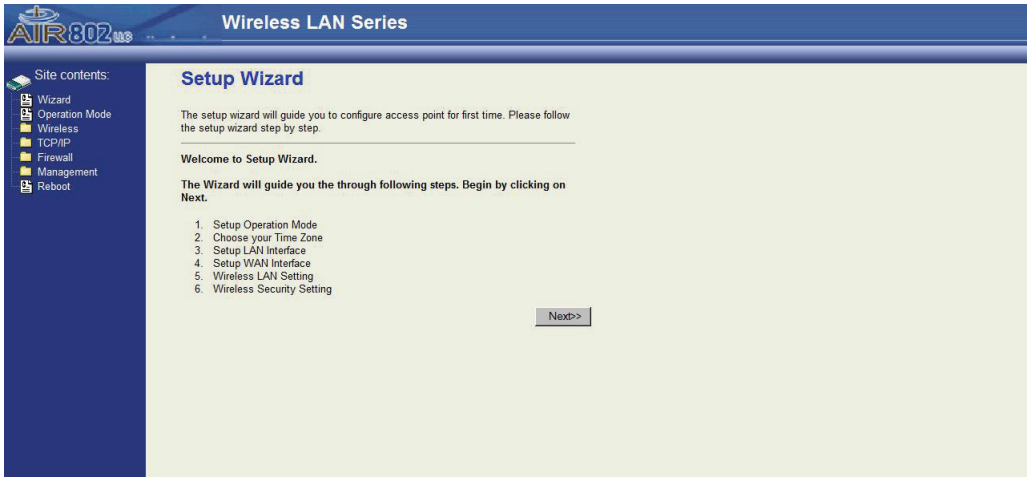
This example is of a basic network between two access points and two computers (could be IP cameras).

For each section, Steps 1-15 below configure the WISP ad hoc mode using the Setup Wizard. Steps 16-19 enable the MESH network.

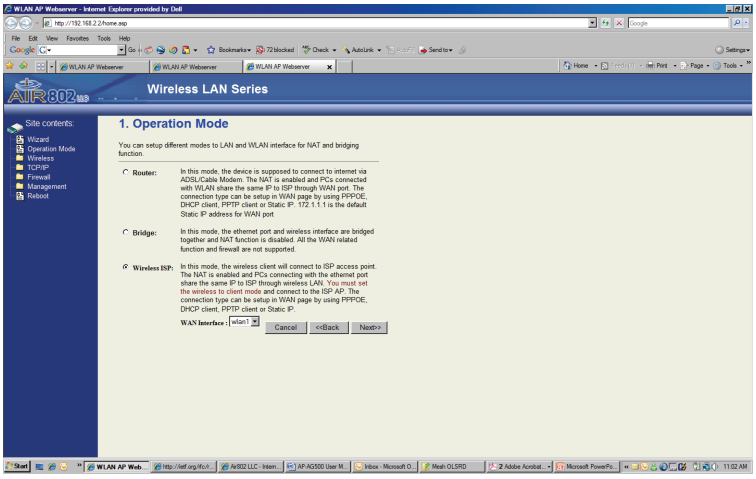
MESH 1

1. Select **WIZARD** in the left panel.

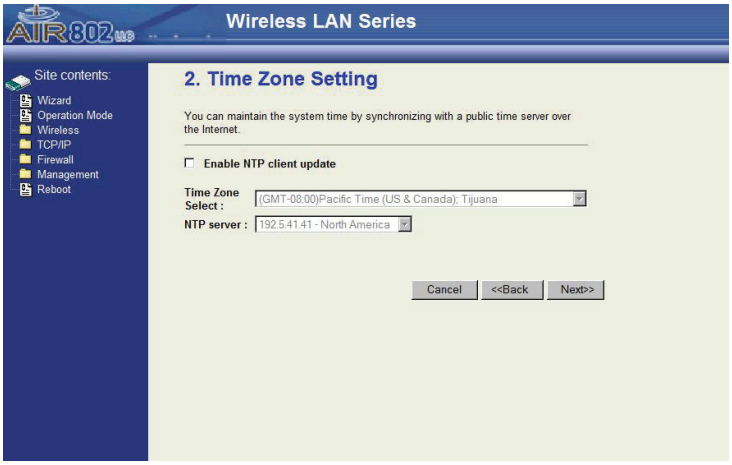
2. Click **Next>>** to continue.


Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Reboot
Setup Wizard
The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.
Welcome to Setup Wizard.
The Wizard will guide you the through following steps. Begin by clicking on Next.
1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting
Next>>

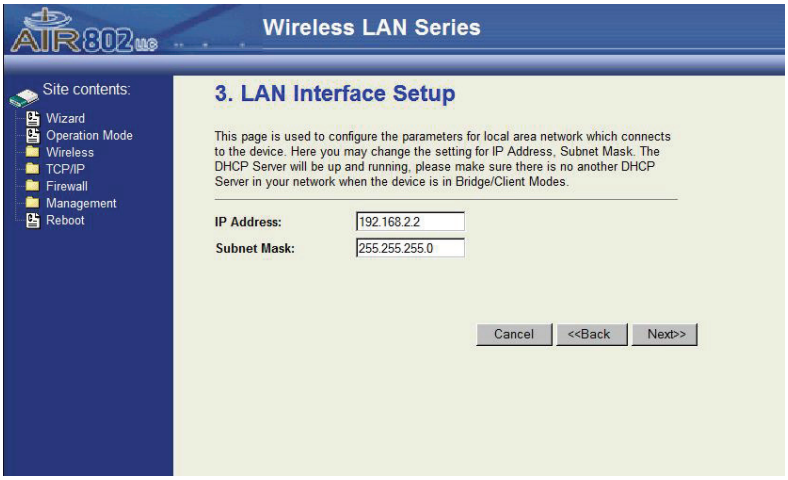
3. Select **Wireless ISP**.
4. Click **Next**>> to continue.



5. Click **Next>>** to continue.

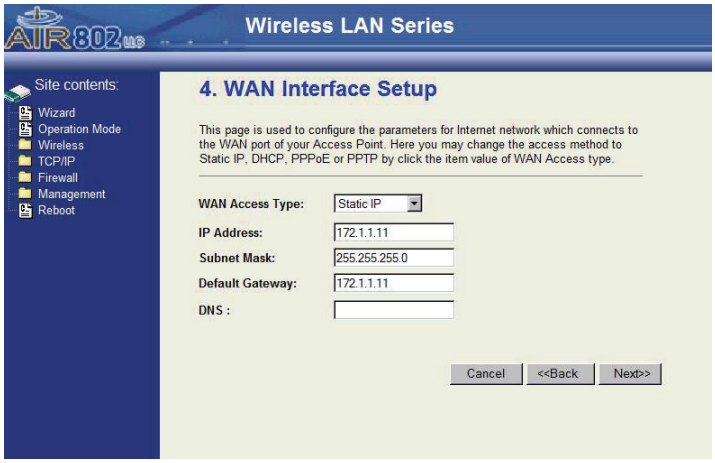


6. Enter the IP Address.
7. Click **Next>>** to continue.


Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Reboot
3. LAN Interface Setup
This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask. The DHCP Server will be up and running, please make sure there is no another DHCP Server in your network when the device is in Bridge/Client Modes.
IP Address:
192.168.2.2
Subnet Mask:
255.255.255.0
Cancel
<<Back
Next>>

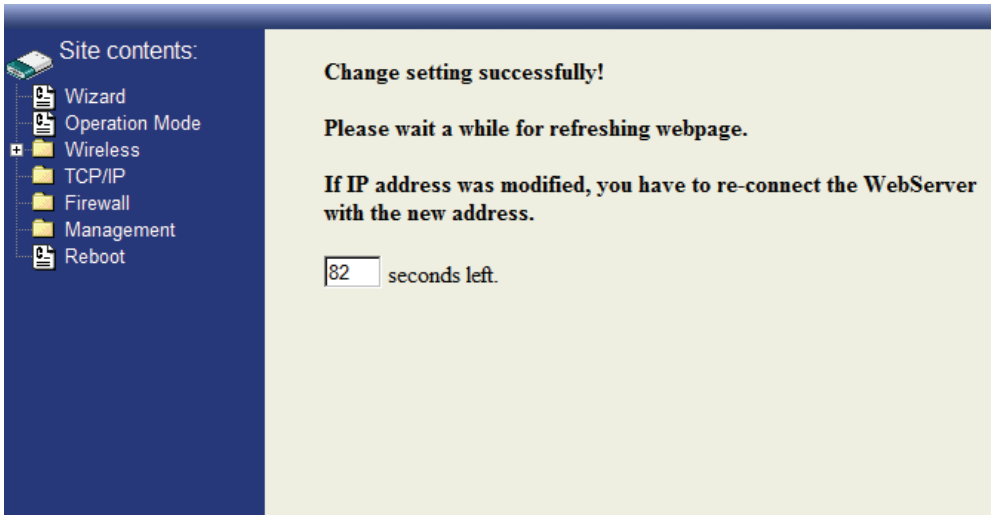
8. Setup the IP Address.
9. Enter the Default Gateway.

10. Click **Next>>** to continue.

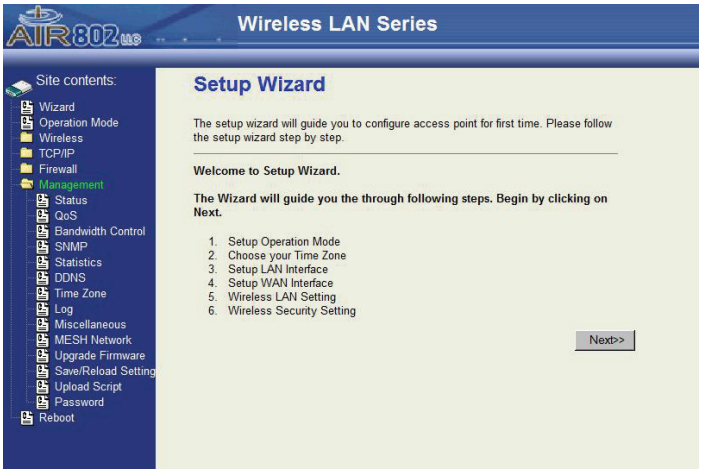

Wireless LAN Series
Site contents:
Wizard
Operation Mode
Wireless
TCP/IP
Firewall
Management
Reboot
4. WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to Static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.
WAN Access Type: Static IP
IP Address: 172.1.1.11
Subnet Mask: 255.255.255.0
Default Gateway: 172.1.1.11
DNS :
Cancel
<<Back
Next>>

11. Select **Ad hoc** mode from the Network Type drop-down list.
12. Enter the SSID.
13. Select Channel 11.
14. Click **Next>>** to continue.

15. Wait for the page to refresh.

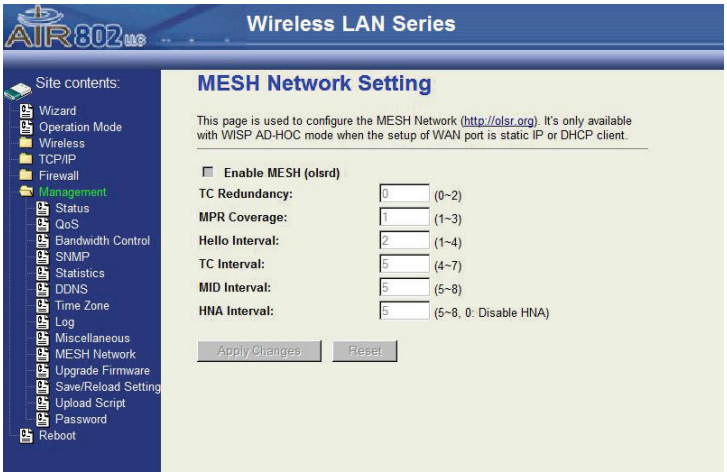


16. Select **Management** in the left panel.



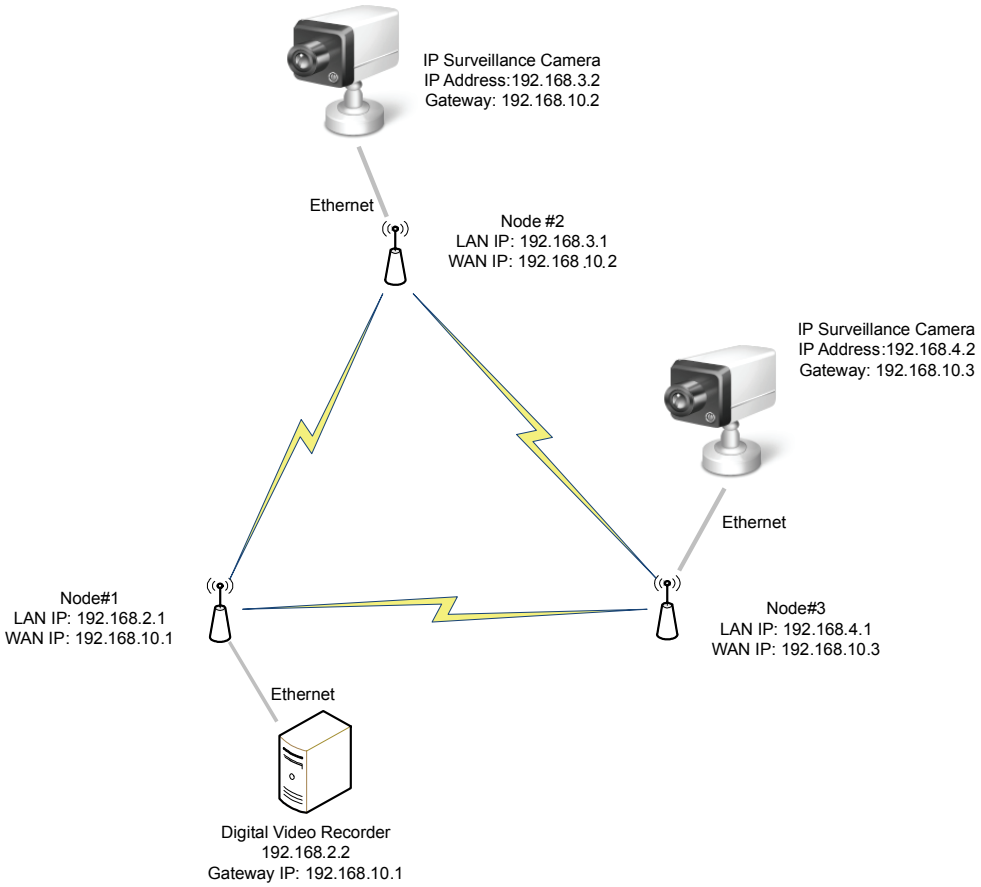
17. Select **MESH Network**.
18. Click **Enable MESH (olsrd)**.

19. Click **Apply Changes**.



EXAMPLE 2

The following represents a basic three-node mesh network for use in an IP video surveillance network.



Upgrade Firmware

Firmware upgrades are made available for download at www.AIR802.com in the Support area.

Firmware Overview

The firmware for the AP-G250 is divided into two files, one containing “webpages” as part of the file name and the other containing “linux”, similar to the following example:

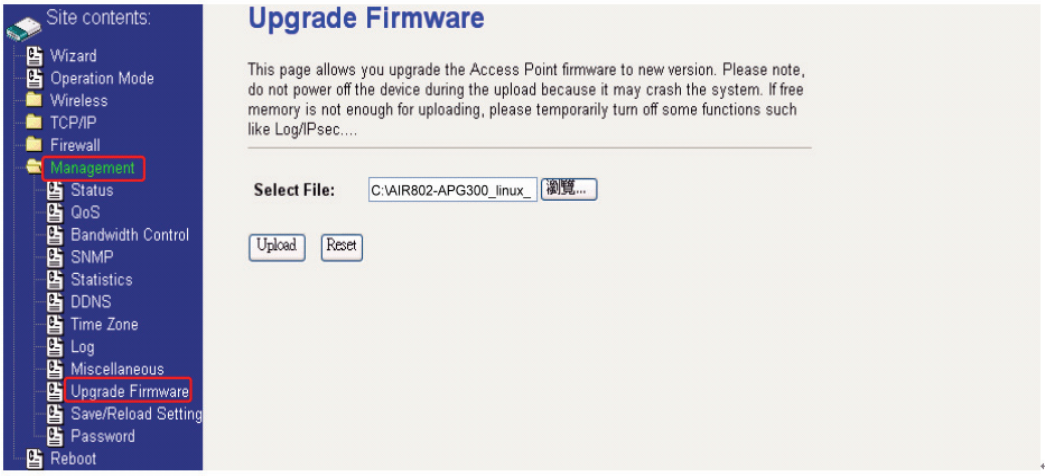
Apg250webpages_adv.bin

Apg250linux_adv_led1.bin

To upgrade the firmware, first upgrade the application firmware (linux file), then the web pages file.

Firmware Upgrade Procedure

The Web-Browser interface is the simplest and safest way to upgrade the firmware. It will check the firmware checksum and signature.



1. Download firmware upgrade files from the Support area at www.air802.com.
2. Click the **Upgrade Firmware** link under **Management** to open the Upgrade Firmware page.
3. Enter the file name of the application firmware file, including the full path, and click **Upload**.
4. Enter the name of the webpages firmware file, including the full path, and click **Upload**.

After upgrading, the AP-G250 will automatically reboot.

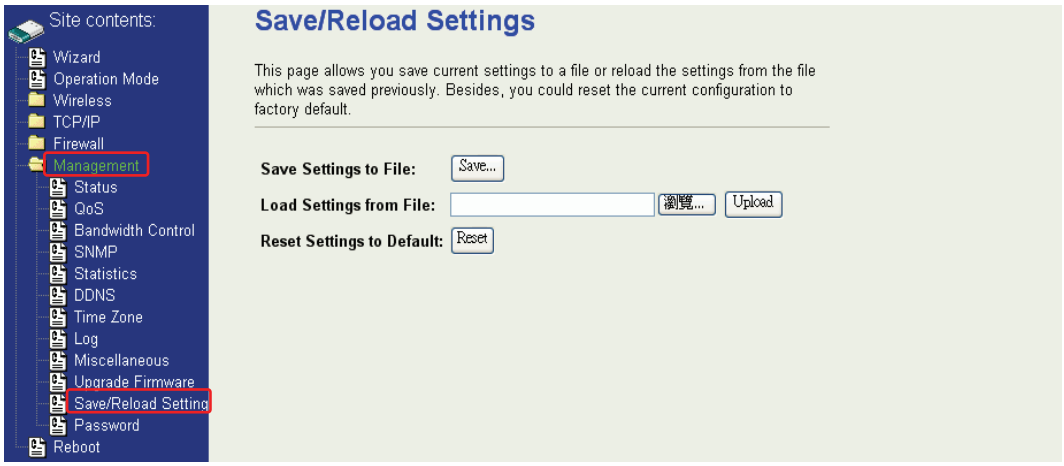
Memory Limitation

Before the system begins a firmware upgrade, it checks to make sure there is enough free memory to upload firmware. If the device lacks enough memory to upload firmware, temporarily turn off some functions and then reboot the device to free enough memory for firmware uploading.

Save/Reload Settings

Reset Settings to Factory Default Values

The AP-G250 can be reset back to factory default settings.



1. Click the **Save/Reload Settings** link under **Management** to open the Save/Reload Settings page.
2. Click **Reset** to return all settings to default values.

In the event that for you can't gain entry to the configuration area, settings can be reset using a switch inside the AP-G250. If you find this necessary, remove the screws around the stainless steel plate at the rear of the unit. Inside, there is a small black pushbutton switch. With the power on, push and hold the pushbutton for 10 seconds. The device will reload all factory default settings (takes one to two minutes).

Saving and Reloading Files

To save a configuration file, click Save and save it to a location in your computer or network. To reload a settings file, enter the file location in **Load Settings From File** and click **Upload**.

Password

To enable password protection for the web-browser interface:

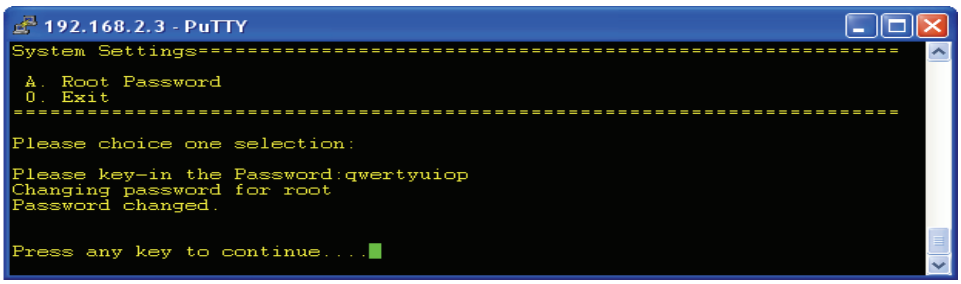
1. Click the **Password** link under **Management** to open the Password Setup page.
2. Enter the User Name.
3. Enter the New Password.
4. Reenter the password in the Confirmed Password area.
5. Click **Apply Changes**.

To disable Web-Browser password protection, remove any entry from the User Name field and click Apply Changes.

USING CLI MENU

Start a SSH (Secure Shell) client session

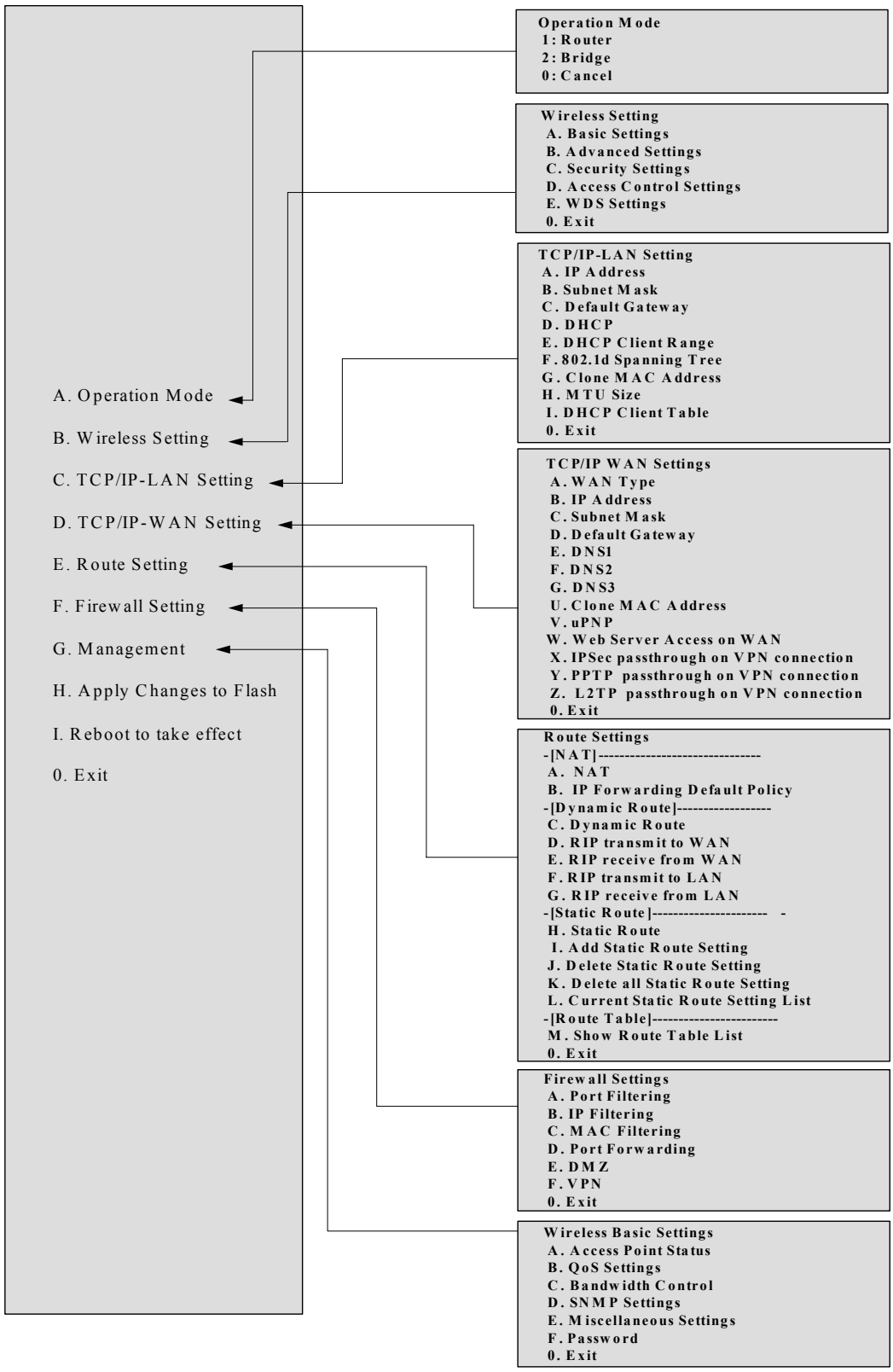
The SSH server daemon inside the AP-G250 uses the well-known TCP port 22. Use a SSH client utility such ad Putty to login to the device. The default user is “root” and password is “zplus12320400”. Once you have logged in to the access point, the password can be changed by CLI command.



Execute CLI program

The CLI program will not execute automatically when you login to the AP-G250. You must manually execute it by typing the case-sensitive command “cli”. Note that any modified settings are not permanently saved until you execute “Apply Changes to Flash” or reboot the access point. The new settings modified by CLI will take effect after rebooting the access point.

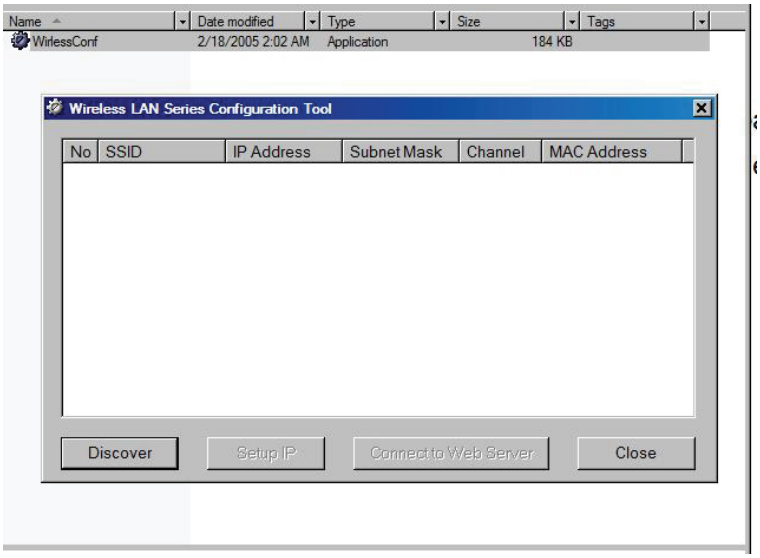
Menu Tree List



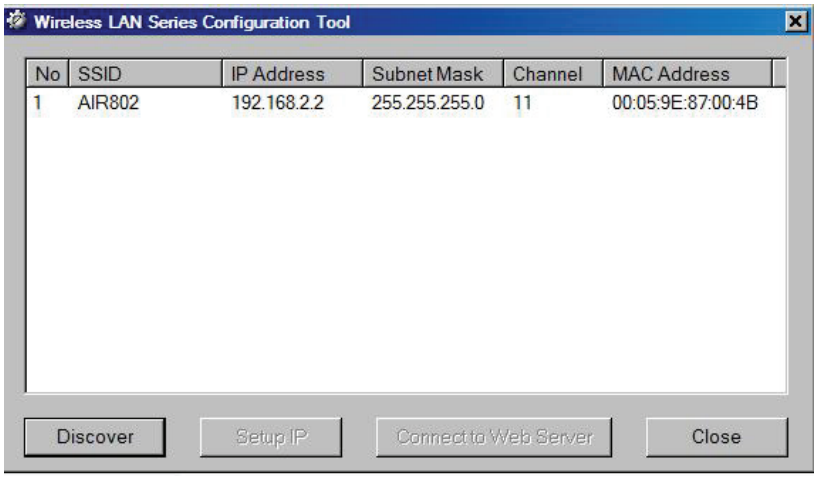
AUTO-DISCOVERY TOOL

Auto-discovery can be used to find any AIR802 access points in your local area network. The tool is named **WirelessConfig.exe** and can be found on the CD included with the AP-G250.

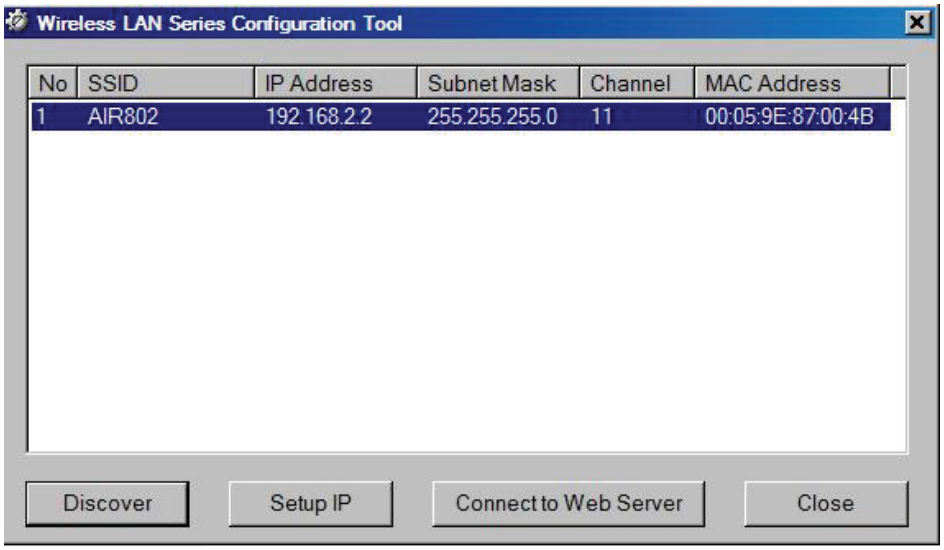
1. Locate the file on the CD and click to open the file. The configuration tool screen opens.



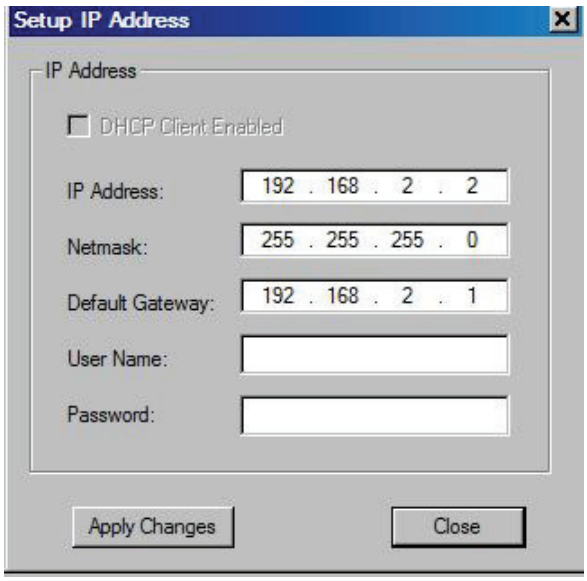
2. Click the Discover button. Any AIR802 access points on the network will appear in the list area.



3. Click once on the desired network. The following screen will appear.



To change the IP address and/or User Name and Password of the AIR802 access point, click **Setup IP**.



If are you on the same subnet, you can connect to an access point by clicking twice on the listing in the discover area or clicking **Connect to Web Server**. Depending on the access point configuration mode, you can access it via the wireless or wired interface.

TROUBLESHOOTING

Basics

After you turn on power to the AP-G250, the following sequence of events should occur:

1. When power is first applied, the Power light (yellow LED) turns on.
2. After approximately one minute:
   - The Ethernet light (green LED) turns on (if a computer/router/modem is connected via Ethernet port).
   - The WLAN light (green LED) begins blinking (except when in WDS Only mode).

Power Light Not On

If the Power and other lights are off, make sure that the power cable is properly connected to the AP-G250 and to a power source. If the error persists, there is a hardware problem and you should contact technical support.

Ethernet Light (LED) Not On

If the Ethernet LED does not light when the Ethernet connection is made, the AP-G250 is not “seeing” the other device. Check the following:

- Ensure that you are using a good, proper cable.
- Make sure that the Ethernet cable connections are securely connected to the access point and at the other end of the cable.

Web Browser Configuration Screen Not Available

If you are unable to access the AP-G250’s Web Configuration interface from a computer on your local network or a directly connected computer, check the following:

- Check the Ethernet connection between the computer and the router as described in the previous section. The AP-G250 Ethernet LED must be on. If the green Ethernet LED is not on, a proper connection does not exist and there is likely a cabling problem.
- Make sure your computer’s IP address is on the same subnet as the AP-G250. If you are using the default addressing scheme of the AP-G250, your computer’s address should be in the range of 192.168.2.1 to 192.168.2.253. Refer to Configuration Preparation in this manual for instructions on how to verify the TCP/IP properties and for instructions on how to configure your computer.
- If you do not know the AP-G250’s current IP address, you can use the “auto-discovery tool” on the CD that comes with the AP-G250. This will discover the IP address whether or not your computer has an IP address on the same subnet. If it is not discovered by our tool or you can’t gain access by typing the IP address

into the web browser URL line, make sure that you do not have a firewall blocking access.

- If you have previously successfully gained access and changed the operation mode to “Router”, you will not be able to access the AP-G250 from the wired interface.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- If you are configuring more than one access point using the same PC, you may encounter an Address Resolution Protocol (ARP) issue. This is due to the access points having the same default IP address but different MAC addresses. If this is the case, try and clear the ARP table of your PC through a DOS command (click Start, click Run, enter CMD in the dialog box, enter arp –d at the prompt and press Enter). Alternatively, you can clear the issue by restarting your PC.
- Try quitting the browser and launching it again.
- If you still can’t gain entry, try a hard reset by pressing down on the reset switch (with power on) for 10 seconds. The unit takes one to two minutes to fully reload the default configuration settings. This will reset the IP address back to 192.168.2.254 if it had been changed.

Configuration Changes Not Saved

If the router does not save changes you have made to the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click Apply Changes before moving to another menu or tab, or your changes will be lost.
- Click the Refresh or Reload button in the Web browser. The changes may have been made but the Web browser is caching the old information.

No Internet Access

Wireless (Bridge - AP Mode)

If you are unable to access the Internet through the AP-G250:

- Verify that you have established a wireless connection between your computer and the AP-G250.
- Unless you are using static IP addresses in your network, verify whether you have been provided an IP address (from the AP-G250 if you are using it as the DHCP Server or from the upstream server, i.e., an existing router). To do this go click Start, click Run, Type CMD in the dialog box and press Enter, type ipconfig at the prompt and press Enter. Scroll up as necessary to see if a valid IP address has been provided. Note: Recent versions of Windows and MacOS will generate and assign an IP address in the range of 169.254.x.x if the computer cannot reach a DHCP server. If the listed IP address is in this range, you have not been

assigned an IP address by the DHCP Server. This indicates a likely issue in the configuration or cabling to an upstream device providing DHCP function.

- If you have enabled encryption (security), access the AP-G250 via the wired Ethernet interface (unless the operating mode is Router). Disable security and re-check to see if you have connectivity. If you do have connectivity, encryption was not properly established between your computer and the AP-G250.
- If your computer has been given a proper IP address, make sure that the IP address is in the same subnet as the IP address of the AP-G250. If it is, click Start, click Run, Type CMD in the dialog box and press Enter. At the prompt, type "Ping x.x.x.x" (where the x's equal the IP address of the AP-G250). You should receive four replies, which indicates that you have a proper connection to the AP-G250. Change your computer's IP address back to the normal setting. You should then be able to "ping" the IP address of any device farther back in the network (another router, modem, etc.). If you are unable to ping a device farther into the network, then you don't have a connection between the AP-G250 and the next device.

Router or WISP Operational Modes

If you have selected Router or WISP as the operational mode, first determine whether the AP-G250 is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your router must request an IP address and obtain one from the ISP.

To check the WAN IP address:

1. Launch your browser and select an external site such as www.air802.com.
2. Access the Main Menu of the AP-G250's configuration at 192.168.2.254 (default) or the current IP address (you many need to change your computer's IP address to the same subnet).
3. Under the Management heading, select **Status**. Scroll down to the WAN Interface area.
4. Check that an IP address is shown for the WAN Configuration. If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, you may need to force your cable or DSL modem to recognize your new router by performing the following procedure:

1. Turn off power to the cable or DSL modem.
2. Turn off power to the AP-G250.
3. Wait two minutes, then reapply power to the modem.
4. When the modem's lights indicate that it has reacquired sync with the ISP, reapply power to the AP-G250.
5. Restart your computer.

If the AP-G250 is still unable to obtain an IP address from the ISP, the problem may be one of the following:

- Your ISP or connection point may require a login program. Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, you may have incorrectly set the login name and password.
- Your ISP can check for your computer's host name. Assign the computer Host Name of your ISP account as the User Name in the WAN Interface menu under TCP/IP.
- If you are connecting to a private network (not an ISP), they may have disabled the DHCP server to prevent unauthorized access or their network might be in non-operating mode.
- Your ISP only allows one Ethernet MAC address to connect to the Internet, and may check for your computer's MAC address. In this case:

  1. Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.

     OR

  2. Configure your router to spoof your computer's MAC address. This can be done in the WAN Interface menu.

If the AP-G250 can obtain an IP address, but your computer is unable to load any Web pages from the Internet:

- You may not have selected **Obtain DNS Automatically** in the TCP/IP folder and WAN Interface page. Verify that this is checked.
- Your computer may not recognize any DNS server addresses. A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer and verify the DNS address as described in "Configuration Preparation" in the beginning of the manual. Alternatively, configure your computer manually with DNS addresses, as explained in your operating system documentation.
- Your computer may not have the router configured as its TCP/IP gateway.
- If your computer obtains its information from the router by DHCP, reboot the computer and verify the gateway address. For details, see "Configuration Preparation" in this manual.
- If the AP-G250 has DHCP Server enabled, you are using client mode, and the IP address provided from the remote AP is in the same subnet as your DHCP address pool, you will have problems. For example, if you have been given an IP address of 192.168.2.10 and the AP-G250 is using 192.168.2.x, then you will need to change the AP-G250 to a different IP subnet, for example, 192.168.5.254.

Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. This makes troubleshooting a TCP/IP network very simple.

Testing the LAN Path to Your Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

To ping the router from a PC running Windows 95 or later:

1. From the Windows toolbar, click Start and select Run.
2. In the field provided, type “ping” followed by the IP address of the router, for example:

   ping 192.168.2.254
3. Click OK.

   You should see a message like this one:

   Pinging <IP address> with 32 bytes of data

   If the path is working, you see this message:

   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx

   If the path is not working, you see this message:

   Request timed out

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
  - Make sure the Ethernet port LED is on. If the LED is off, follow the troubleshooting instructions “Ethernet Light (LED) Not On” earlier in this section.
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) connected to your workstation and router.
- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
  - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device. From the Windows run menu, type:

PING -n 10 <IP address>

where <*IP address*> is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information will not be visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway.
- Check to see that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the User Name in the WAN Interface menu.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized computer. To do this, click on the WAN Interface link under the TCP/IP heading of the browser interface at *192.168.2.254*, and enter the authorized computer's MAC address under "Clone MAC Address".

APPENDIX A

Technical Specifications

WLAN Standards

- 802.11b
- 802.11g

Radio Scheme

- 802.11g: OFDM (64QAM, 16QAM, QPSK, BPSK)
- 802.11b: DSSS (CCK, DQPSK, DBPSK)

Frequency Range

- 2.4 ~ 2.497 GHz

Operating Channels

- 11 for North America
- 13 for Europe
- 14 for Japan

RF Output Power Stepping

- 802.11b: 20dBm (100mW) ~24dBm (250mW) @ 11 Mbps
- 802.11g: 17dBm (50mW) ~20dBm (100mW) @ 54 Mbps

Sensitivity

- 802.11b: -84 ±2dBm @ 11 Mbps
- 802.11g -71 ±2dBm @ 54 Mbps

Data Rate

- 802.11g: 54/48/36/24/12/9/6 Mbps
- 802.11b: 11/5.5/2/1 Mbps

Operating Mode

- Router (NAT enabled)
- Bridge
- WISP (AP Client with Routing Function – NAT enabled)

Wireless Modes

- Access Point

- Access Point + WDS
- WDS (Wireless Repeater, Point-to-Point, or Point-to-Multipoint)
- Client Device (Ethernet to WLAN Bridge)
- Universal Repeater Mode (AP Client + AP Functionality Simultaneously)

Wireless Features

- MAC Clone (Client Mode Only)
- Access Control (Allow or Deny Client MAC Addresses)
- Site Survey (Scan Wireless Networks)
- AIM Tool (Fine Tuning Antenna Direction)
- Show Active Associated Clients

Wireless Features – Advanced

- Authentication Type (Open System, Shared Key, Auto)
- Fragmentation Threshold Adjustment (256-2346)
- RTS Threshold Adjustment (0-2347)
- Beacon Interval Adjustment (20-1024ms)
- ACK Timeout Adjustment (0-255, 0 is default)
- Client Expiration Time (101-40000000 Sec)
- MTU Size Adjustment (100 to 1500)
- Data Rate Selection (Auto or Rate Interval)
- Preamble Type (Long or Short)
- Broadcast SSID (Enable or Disable)
- IAPP [IEEE 802.11f Station Roaming within Subnet (Enable or Disable)
- 802.11g Protection – Protects 802.11b Users (Enable or Disable)
- Block WLAN Relay Between Clients (Enable or Disable [auto])
- Turbo Mode [Applies to Realtek WLAN Chipsets] (Enable or Disable)
- Aggregation Mode (Enable or Disable)
- Tx Burst Mode (Enable or Disable)
- Transmit Power – OFDM (802.11g) Step Down Adjustment
- Transmit Power – CCK (802.11g) Step Down Adjustment

Security

- Password Protection
- Encryption [None, WEP, WPA(TKIP), WPA2(AES), WPA2(Mixed)]
- MAC Filtering
- Hidden SSID Broadcast

- 64/128-bit WEP Encryption
- WPA for 802.1x and WPA-PSK
- WPA2 / IEEE 802.11i
- WPA Authentication Mode [Enterprise (RADIUS), Personal (Pre-Shared Key)]

LAN Interface

- Set IP Address, Subnet Mask and Default Gateway
- Set DHCP (Server, Client, Disabled)
- Set DHCP Client Address Range
- 802.1d Spanning Tree (Enable or Disable)
- Clone MAC Address
- Set MTU Size

WAN Interface

- Set WAN Access Type (Static IP, DCHP Client, PPPoE, PPTP)
- Set IP Address, Subnet Mask and Default Gateway
- DNS (Automatic or Manual Entry)
- Clone MAC Address
- Enable uPnP
- Enable Web Server Access on WAN
- Enable IPsec pass through on VPN Connection
- Enable PPTP pass through on VPN Connection
- Enable L2TP pass through on VPN Connection

Routing

- NAT (Enable or Disable)
- IP Forwarding Default Policy (Accept or Decline)
- Dynamic Routing (RIP v1 & RIPv2) or Static Route

Firewall

- Port Filtering
- IP Filtering
- MAC Filtering
- Port Forwarding
- DMZ (Demilitarized Zone)
- VPN

Management

- Status (Firmware Load, Current WAN/LAN IP Address and More Info)

- QoS Enable & Set Parameters
- Bandwidth Control (Set Upstream & Downstream Rate in Client Mode)
- SNMP (Enable or Disable and Set Parameters)
- Dynamic DNS Service (Enable or Disable and Set Parameters)
- Time Zone (Enable NTP Client)
- System Log
- Misc (Set HTTP Port, RSSI Interval, Enable Ping Watchdog)
- Mesh Network - Optimized Link State Routing Protocol (OLSR)

  Available in WISP AD-HOC Mode if WAN Port is Static IP
- Firmware Upgrade
- Save/Reload Settings to Hard Drive
- Web GUI
- SSH
- Discovery Tool (discovers IP address)

Antenna

- RP-SMA Jack (Female) Connector
- 3dBi Dipole Antenna

Power Supply

- DC 5VDC

Operating Environment

- Temperature 32° to 122°F (0° to 50°C)
- Humidity 10~90% (non-condensing)

Certificate

- FCC, RoHS

APPENDIX B

Basic Wireless Bridged Access Point

The settings below are the general basic requirements for a bridged AP. This generally implies that you will be connecting the AP-G250 into an existing router or switch.

Operating Mode: Select Bridge unless you are directly connected to a cable or DSL modem) or you have other network architecture requirements.

Wireless Mode: Select AP (under Wireless Folder, Basic Settings).

DHCP Server: Under TCP/IP Folder, LAN Interface, change the setting to either Disabled or Client (if you already have a DHCP server in your network, i.e., if you are plugging the AP-G250 into an existing router).

Basic Wireless Router

The settings below are the general basic requirements for configuring as a wireless router. This generally implies that you will be connecting the AP-G250 into a cable or DSL modem.

Operating Mode: Select Router.

Wireless Mode: Select AP (under Wireless Folder, Basic Settings).

WAN Interface Type: Under TCP/IP Folder, WAN Interface, change the setting to DHCP Client if your ISP provides a dynamic IP address. Also you will likely need to select “Attain DNS Server Automatically” if you have not been provided a DNS server IP address.

Universal Repeater Mode

The settings below are the general basic requirements for configuring the AP-G250 as a universal repeater. This implies that you will connect to another wireless AP/router’s SSID and rebroadcast within your area.

Operating Mode: Select required mode. Otherwise leave at default (Bridge mode).

Wireless Mode: Leave under default AP mode.

Universal Repeater Mode: Under the Wireless folder, Basic Settings, check Universal Repeater mode. Click the Refresh button to view available networks. Type the SSID of the desired network into the Extended SSID field and click Apply Changes at the bottom of the page.

WDS or WDS+AP Mode

The settings below are the general basic requirements for configuring the AP-G250 with WDS alone or WDS+AP. The WDS function allows multiple access points to be networked together via wireless. If you do not require an SSID to be broadcast and no users will connect via wireless, then select WDS. If you need the AP to also simultaneously act as an access point providing wireless service, then select WDS+AP. Up to eight access points can be connected together in WDS. To use WDS, you must be in control of all access points and know their MAC addresses.

Operating Mode: Select Router or Bridge mode as required normally Bridge mode).

Wireless Mode: Select WDS or WDS+AP as required.

Setup WDS: In the Wireless folder, select the WDS Settings page. Click the box to enable WDS. Carefully enter the MAC address of any far-end AP that will be directly communicating with this AP. Each AP has two MAC addresses. You are entering the wireless MAC address (or MAC1 on the physical label). If the MAC address is not entered correctly, the WDS bridge will not work.

DHCP: Under TCP/IP, LAN Interface, change DHCP from Server to Disabled or Client (if a DHCP server already exists on the network).

Client Mode

The settings below are the general basic requirements for configuring the AP-G250 as a client device. Using the AP-G250 as a client device can be thought of as essentially having a powerful WiFi card in your computer. You can survey (under Wireless folder, then Site Survey) all available networks and connect to them. They are shown with details such as the SSID, channel number, if they are encrypted or not and information about the quality of the signal.

In this mode, the wireless connection is used for connecting to the remote AP/router. Your local network will be wired. It could be wired to another wireless router if desired.

Operating Mode: Select Bride or WISP mode. If you are using a single computer behind the AP-G250, leave it in the default Bridge mode. WISP mode is a routed mode with NAT enabled. This is useful if you are connecting multiple computers behind the AP-G250.

Wireless Mode: Select Client

WAN Interface: Under TCP/IP folder, select the WAN interface page and change the WAN type from Static IP address to DHCP Client.

AIR 802 LLC